Security Architecture for Mobile E-Health Applications in Medication Control

Fábio Gonçalves
Centro Algoritmi
University of Minho
a44031@alunos.uminho.pt

Joaquim Macedo
Centro Algoritmi / DI
University of Minho
macedo@di.uminho.pt

M. João Nicolau
Centro Algoritmi / DSI
University of Minho
joao@dsi.uminho.pt

Alexandre Santos*
Centro Algoritmi / DI
University of Minho
(*corresp. author) alex@di.uminho.pt

***Abstract*—The use of Radio Frequency Identification technology (RFID) in medical context enables not only drug identification, but also a rapid and precise identification of patients, physicians, nurses or any other health caregiver. Combining RFID tag identification with structured and secured Internet of Things (IoT) solutions enable ubiquitous and easy access to medical related records, while providing control and security to all interactions.**

This paper defines a basic security architecture, easily deployable on mobile platforms, which would allow to establish and manage a medication prescription service in mobility context making use of electronic Personal Health Records. This security architecture is aimed to be used with a mobile e-health application (m-health) through a simple and intuitive interface, supported by RFID technology. This architecture, able to support secured and authenticated interactions, will enable an easy deployment of m-health applications. The special case of drug administration and ubiquitous medication control system, along with the corresponding Internet of Things context, is used as a case study.

Both security architecture and its protocols, along with a general Ambient Assisted Living secure service for medication control, is then analyzed in the context of the Internet of Things.

***Keywords*—Security Protocols, Cryptography, RFID, Internet of Things, Ambient Assisted Living, Personal Health Records**

I. Introduction

A problem that the health services in Portugal have, and also plenty of other countries,is their growing costs, specially when imply specialized care support in health centers and hospitals. As a consequence of health care large costs, whenever possible, many health services are being relocated from hospitals to the patient's home. In order to assure no loss on the quality of the health services, automated and semi-automated tools must be used.

From the moment in which the medication is prescribed, by the physician, until it is administrated to the patient plenty of mistakes can happen. These can occur due to a misinterpretation of the communication (either written or oral) [1] or to errors made by the patients themselves when taking the drugs. The patient must take the right dosage of the right drug at the right time and this may be controlled by secure access to the patient's Personal Health Record (PHR).

In outpatient clinic, most of people take the medication without any medical or other specialized assistance, increasing the likelihood of errors occurrence, mainly with elderly patients [2]. To assist this process of medication intake, several existent technologies may help, as long as the associated security risks can be minimized. Using the pervasive Internet, information can be accessed anywhere; using automatic identification of all participants, processes may be (semi-) automated and error may be strongly reduced. Undoubtedly, both life and heavy financial risks may arise when security is compromised. So, most e-health related applications must enforce strong security procedures, in order to avoid wrong treatments, wrong identifications or unauthorized access. Furthermore, a log record of all significant events must exist, so that any heath caregiver negligence may be detected.

The Radio-Frequency IDentification, commonly known as RFID, is used in many applications [3], [4]. The use of this technology is constantly evolving and is expanding at exponential rate. There are several methods of identification, although the most common is a microchip able to store a serial number that identifies the person, object or thing. Using electronic devices that emit radio frequency signals, it is possible to perform an automatic capture of data (in this context called a tag [5]), from a reader. Therefore, RFID is an acquisition information technology that enables auto-identification.

The use of Internet to carry information contained in tags is commonly known as "*Internet of Things*" [6], [7]. This term is defined as objects carrying identity and virtual personality, which, while working in intelligent spaces, use interfaces to connect and communicate in a social, environmental and personal context.

This work analyzes and presents new security protocols and solutions to integrate in the m-health service architecture [8], where a remote medication control system for Ambient Assisted Living, specially aimed at elderly people, is proposed.

Using available technology (self-identification, encryption and Internet of Things [9]), it is intended to define and evaluate components with strong security restrictions both in terms of identification and authentication, at storage and transmission levels. These components are combined within a security architecture designed to manage a m-health prescription and monitoring service adapted to an ubiquitous access in mobile environments.

A. Motivation

As already mentioned, one of the main objectives of the security architecture for health services rendering in mobility context, is to avoid errors in medication intake. This is particularly important in an outpatient setting and it must be done in a easy and also strongly secured way, without very specialized assistance.

In fact, a study carried out in Portugal on *"Adherence to Medication Regimen in the Elderly"* [2] (PhD thesis, in Portuguese) showed that a large majority of the elderly people need external help for managing medication. Having carried out a study with a population of elderly people, the study [2] stated *"as part of the reasons for non-adherence to medication, 60.5% of the patients indicated forgetfulness and 24.4% stated they did not have them with them at the time of intake"* and *"interventions (giving advise on drugs, drugs control and drug education) are effective in increasing adherence"* to medication.

TABLE I. ELDERLY TYPE OF HELP NEEDED (ADAPTED FROM [2])

Help Needed	Number	%
Manage Medication	119	36,1
Get Info on Medication	63	19,2
Explain Medication regime	44	13,3
Interpeter Medication regime	26	7,9
Monitor Medication regime	20	6,1
Remembering Medication Hours	19	5,8
Filling Drug-dispenser	10	3,0
Monetary Help	7	2,1
Reading Label	8	2,4
Get Drugs Out of box	4	1,2

As one can notice, a large majority of the elderly need help in medication control, being that 82.8% point out reasons where semi-automated AAL systems may be of invaluable help.

B. M-Health Application Scenario

In [8], an e-Health Service is proposed, whose main goal is to develop a simple m-health service for AAL, based on RFID and IoT technologies. The main objective of the security framework presented in this paper is the establishment of a secure architecture and access control to the information system relating patients, prescriptions and medications, in order to easily verify, specially when in mobility, the compliance by patients of the prescribed medications and dosages. This m-health service for AAL assumes that physicians, patients and medicines are to be identified by means of RFID-tags and that the whole process, from prescription to pharmaceutical drug administration, is to be monitored by means of an IoT-based information system. The whole process begins at a health facility when the physician prescribes a set of pharmaceutical drugs to the patient, being both the physician and the patient identified by means of RFID-tags. These tags are enablers of the establishment of an IoT architecture and access control mechanisms to the information system relating patients, prescriptions and medications.

It is assumed that physicians fill out the prescription where they include the dosage and time when the medication shall be taken. This information is stored into the e-health system database, already linked to the RFID tag assigned to each patient. These tags can be read by RFID readers placed in any specific hardware but also (and specially) by means of readers attached to general purpose mobile devices, such as smart phones, tablets, PDAs, etc.

In such a context, as depicted in Figure 1, the patient will have a smartphone (or a tablet) running the m-health application. Physicians, using their own personal or institutional devices (either mobile or fixed) will issue prescriptions that will be immediately updated in the database. Patients' mobile device will access that database and will update the medical recommendations that can be downloaded in order to be used in offline mode. Mobile devices, using RFID technology, enables pharmacists to deliver the right medication to users and enable users to verify that they taking the right medication at right time. Along this whole process, the security is a major concern: data confidentiality and integrity must be assured, users and even applications authentication must be verified.

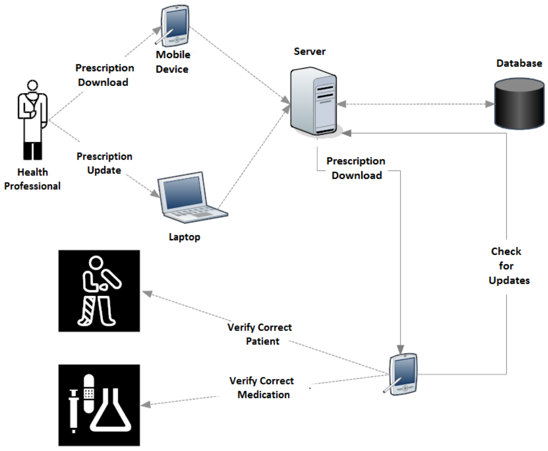

Fig. 1. M-Health Application Scenario

II. RELATED WORK

Several studies on Ambient Assisted Living (AAL) to support elderly people in their daily routine have already been published, either from Dohr et al [10] presenting smart objects to facilitate generic tele-monitoring processes, or from Chun-Liang et al [11] with a framework for using RFID patient identification within the Taichung Hospital information system. More recently, other works such as RMAIS [12] have studied the integration of medication with patients and even some hardware products, such as special medication dispensers, arose [13]. These works rely on special hardware devices, either sensors for tele-monitoring, or special dispensers to interact with patients.

Another important related work is the service architecture that will be used as the basis for work presented in this paper, which is the e-health service architecture and components proposed in [8].

Figure 2 presents its prototype, starting from the moment an RFID tag is read and ending with the resolution of the Electronic Product Code (EPC) [14], [15] information, taken from an Object Name Service (ONS) [16] server. Results taken from the Object Name Service will serve as indexing mechanism to e-health information databases. This service prototype, developed in Java language, has been set fully operational (complete details can be found in [8]). To support general ONS requests several Java classes were developed in

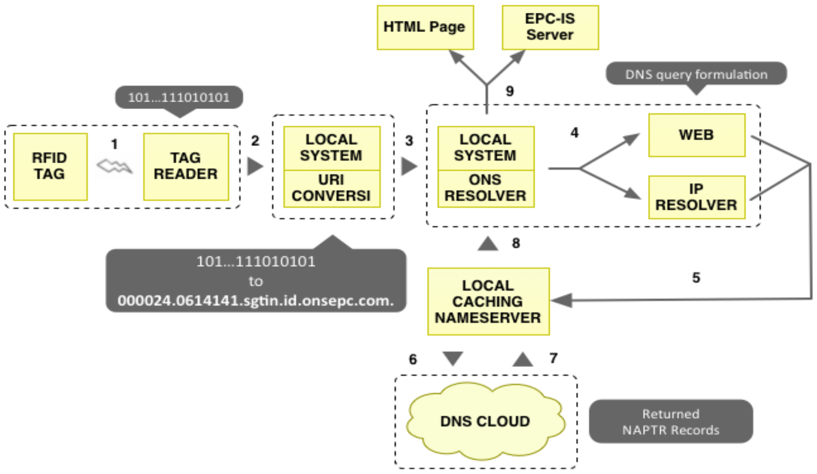

Fig. 2. Schematic of the m-health prototype with ONS resolution (based on [16])

order to read EPCs, perform lookup queries to the ONS service and access the information databases.

That initial prototype, apart from using SSL and HTTPS, did not yet include any special security mechanisms. It is imperative to make this e-health service safer. Therefore, it is essential to have a security mechanism with strong authentication, able to record the time and the user identification of all accesses. This enables fraud detection for any system flaw.

There already exists security architectures for e-health services such as [17]. Unfortunately, such architectures seem to be too heavy to be used in mobile environments, where devices have limited capabilities and intermittent network connections.

Of course one should protect both the access to the RFID data, the access to all the ONS services, and finally the access to the m-health application and services. For all client - server interactions, strong authentication (e.g. by using host digital certification) should be used.

A. *Security in Internet of Things (IoT)*

To exchange secret information over the Internet, it is necessary to secure the channel before doing so. The security may be applied into the different layers of the TCP/IP model.

The usual methods to provide security at the network level, in the case of packet networks, is datagram encapsulation [18]. One of the most common technologies used to ensure secure communications in the Internet is the Internet Protocol Security (IPsec) protocol suite. IPsec is an end-to-end security scheme operating in the IP stack, enabling both authentication and confidentiality. Although IPsec ensures these security services to any protocol in the upper layers, it introduces some overhead that will reduce throughput.

At the transport layer, the Secure Socket Layer (SSL) protocol is the standard used all over the Internet. According to [19] the SSL protocol replaces the TCP/IP sockets with SSL sockets , simplifying the implementation of a secure end-to-end secure channel. This approach reduces the implementation time comparing with the time spent designing another cryptographic system with the same security level. SSL protocol supports many cipher types that can be used in operations such as client or server authentication, exchange certificates or establish session keys. As evolution of SSL there is now the Transport Layer Security (TLS) [20], with new versions and some security extensions.

Although SSL provides a very good solution, it authenticates only the machines in both ends, not the applications nor the users. So a rogue application may try to attack the server by impersonating a trusted application. Another problem may be caused by a virus, able to replace the SSL sockets and capture all the exchanged information, in clear text. Taking this problems into account, along with the security flaws in health context, we think that security must be applied also at the application layer. So, as no normalized and standard protocol has been yet released, a new application layer security protocol will be presented to be used in m-health context.

B. *Security in Radio Frequency Identification (RFID)*

There are several types of tags to be used in RFID, which can vary in many features such as cryptographic primitives, processing capacity, memory, passive or active. These RFID tags can be divided in four classes, which are show in Table II.

TABLE II. TAG CLASSES

Class	Tag Type	Characteristics
Class 1	Identification tags	EPC, tag ID, optional user memory
Class 2	Extended Identification tags	Bigger ID, Bigger User memory
Class 3	Battery assisted passive Tags	Energy source, Optional data log
Class 4	Active tags	Add communications over an autonomous transmitter

Almost all studied protocols for securing communications on RFID are using tags that comply with the standard EPC Gen2 [21] (EPC Class-1 Generation-2 UHF RFID). These tags are low cost and their use enables building an average cost system able to offer a suitable level of security, especially regarding the protection of privacy [22].

According to [23] security attacks on RFID may be classified into three main categories: privacy and authentication attacks, attacks on data integrity and the network availability attack (Denial of Service (DOS) attacks). The most relevant protocols to be used with RFID found in literature were RFID Grouping Proofs [24] and Cryptographic Puzzles [25].

C. Cryptography and Security

The main objective of cryptography [26] is to achieve confidentiality, integrity, data origin authentication, entity authentication and non-repudiation.

Tools such as hash [19] functions, digital signatures [27], symmetric and asymmetric keys [27], and public key certificates, are needed to achieve these features. Public key certificates are documents that prevent the use of a forged key to impersonate another entity [19]. Certificates are issued by an Certification Authority, CA, any trusted central administration that is willing to testify the validity of the certificates issued.

Most of the cryptographic operations mentioned do not require an Internet connection; for example, the authenticity of a certificate may be verified offline. As the certificate has the CA public key and is signed by it, the only information that the application needs to know is the validity of the CA public key. Once the validity is checked, it can verify the certificate's authenticity and the authenticity of all messages signed with the public key in the certificate (but, generally, the Internet connection may be needed to exchange keys or certificates).

III. Security for Mobile E-Health Applications

A. M-Health Security Context

The health environment is very sensitive, and so it has some very specific security requirements. It is necessary to prevent any unauthorized access attempt to private information and it is also important to keep an updated log that records system failures [8].

In a health environment system is important to balance system security with availability. A non authorized access may be harmful to the system or patients, but in case of emergency if medical personal can't reach the needed information it can be even more dangerous, mainly to the patients. Keeping this in mind, we propose the creation of two types of access: one with read-only permission and another with a read-write permission. In this scheme, security may be a little more relaxed in the read only access, making the information more easily available. In the read-write access, the security is more strict because adding or altering important information may be catastrophic, either financially or even to patients lives.

All the patient's information to be accessed is assumed to be manageable in the context of a patient's electronic Personal Health Record (ePHR). According to definition from the *Healthcare Information and Management Systems Society* an electronic Personal Health Record (ePHR) [28] is a *"[...] lifelong tool for managing relevant health information, promoting health maintenance and assisting with chronic disease management via an interactive, common data set of electronic health information and e-health tools. [...] The ePHR is owned, managed, and shared by the individual or his or her legal proxy(s) and must be secure to protect the privacy and confidentiality of the health information it contains"*.

The IT system supporting the patient's ePHR is to be accessed by health professionals and patients. The patients will be given a mobile device from where they will access the system and their ePHR. The health professionals will be able to access the system with a mobile device or a laptop.

A read-only access will be made possible with the device either connected or disconnected to the Internet, but the read-write access will always require an Internet connection on account of the (strong) authentication protocol proposed in this paper. All the accesses to the ePHR must be auditable, maintaining a robust log that clearly identifies the user, time of occurrence and associated data operation performed.

Also, all the communications between the RFID tags and readers will make use of a secure protocol, such as the Grouping Protocol proposed by [22] or the cryptographic puzzles proposed by [25]. The protocol proposed by [22] should be more appropriate to apply in this case, mainly for establishing the association between medication-prescription-patient, once it was designed by [22] with that purpose. On the other hand, to exchange the tag ID with the application for authentication purposes, the protocol proposed by [25] is certainly more suitable. With this new approach by [25] to the RFID security, the tags generate a puzzle for the reader to solve, making use of a time bounding protocol that increases the puzzle difficulty with the increasing of the tag-reader distance.

B. M-Health Security Protocol

A new security protocol aimed at mobile e-health applications, identified as M-Health Security Protocol (MHSP), is proposed and presented within this section. The proposed protocol (cf Fig. 3) finds its roots on the well known SSL protocol. Instead of using it in the traditional transport layer, MHSP was aimed at the application layer. This choice was made due to the great security provided by the SSL, noticing also that SSL is widely used in the global Internet.

This protocol provides a secure channel over the Internet and authentication between the applications. The authentication between applications is achieved using Public Key Certificates. This certificate can be verified by a Certificate Authority (CA).

Following, it will be explained in detail the proposed MHSP protocol. Will be assumed that $CApp$ is the client application and S is the server's application, CC the client application certificate and SC server certificate. The message with order n exchanged between entities is represented by m_n and RN the random data with order N generated by the application. Likewise $enc(M, K)$ is the ciphering of the message M with key K and $dec(M, K)$ is the opposite operation. S_{pubKey} and $S_{privKey}$ are the server's public and private key, the same happens with $CApp_{pubKey}$ and $CApp_{privKey}$, but in this case are the client's keys. Finally $gen(key)$ generates the desired key.

1) The client application sends its own certificate to the server.
   $CApp \rightarrow S : CC$

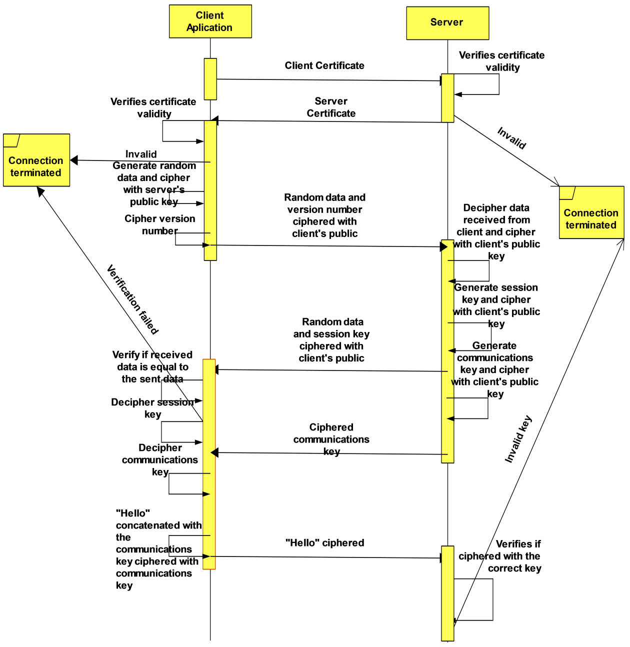
Client Aplication
Server
Client Certificate
Verifies certificate validity
Verifies certificate validity
Server Certificate
Invalid
Connection terminated
Invalid
Generate random data and cipher with server's public key
Cipher version number
Random data and version number ciphered with client's public
Decipher data received from client and cipher with client's public key
Connection terminated
Verification failed
Generate session key and cipher with client's public key
Random data and session key ciphered with client's public
Verify if received data is equal to the sent data
Generate communications key and cipher with client's public key
Decipher session key
Ciphered communications key
Invalid key
Decipher communications key
"Hello" concatenated with the communications key ciphered with communications key
"Hello" ciphered
Verifies if ciphered with the correct key

Fig. 3. M-Health Security Protocol (MHSP) interactions

2) The Server Application verifies the validity of the received certificate, terminating the connection if not verified.

```
if ($CC$ is invalid)
   then Connection terminated
else $S \rightarrow CApp : SC$
```

3) The Client Application verifies the validity of the received certificate and if is invalid, the connection is terminated. Otherwise it will generate a challenge so it can verify the server authenticity.

```
if $SC$ is invalid
   then Connection terminated
else $m_1 = enc(< V, R1 >, S_{pubKey})$
     $C_{App} \rightarrow S : m_1$
```

4) In this phase the server will have to prove his authenticity to the client using the challenge received. Then it will generate the session and communications keys.

```
$< V, R >= dec(m_1, S_{privKey})$
$gen(Sess_{key})$
$m_2 = enc(< R1, Sess_{key} >, CApp_{pubKey})$
$S \rightarrow CApp : m_2$
$gen(Comm_{key})$
$m_3 = enc(Comm_{key}, Sess_{key})$
$S \rightarrow CApp : m_3$
```

5) With the reply the client application can verify the servers authenticity and obtain the session and communications keys

```
$< R1, Sess_{key} >= dec(m_2, C_{priv_{key}})$
if $R1_{sent}$ equal $R1_{received}$
   then $Comm_{key} = dec(m_3, Sess_{key})$
        $gen(R2)$
        $m_4 = enc(< "Hello", R2 >, Comm_{key})$
        $CApp \rightarrow S : m_4$
else Connection terminated
```

6) Finally the server will decipher the message m_4 sent by the client application and, if deciphered correctly, it means that the client application was able to decipher the $Comm_{key}$ correctly and the is authenticated.

```
if $dec(m_4, Comm_{key})$
   then Authenticated
else Connection terminated
```

Previously are mentioned two symmetric keys: session key and communications key. To make sure each key isn't used too many times, the session key is used to cipher the communications keys. Only the communications keys will be used to communicate between applications. Thus, since the communications keys are always changing, even if an attacker discovers one key it will only work for a short period of time. The purpose of "Hello" message sent with the random data ($R2$) is to make the result from $enc(< "Hello", R2 >)$ always different.

The cipher algorithm to be used will be pre-defined and may vary according to the version of the protocol. This way the server will be able to identify which cipher algorithm the client application is using by its version number. The server may refuse the connection if the algorithm used in that version is not secure enough.

C. User Authentication in M-Health Context

In order to solve the authentication problem in e-Health context for medication control, were proposed two possible scenarios: one for prescription writing (read-write operations) and another one for prescription consultation (read-only operations); these scenarios will be identified by Secure User authentication (SUA) and User Authentication (UA), respectively. For both methods it is assumed that the user authentication protocol will make use of the communication channel already established and secured with the MHSP (presented in section III-B). Before presenting the authentication protocols it is necessary to define the registration process of each user.

1) Registration process: The registration must be done by an entity trusted by the system (CA). The registration for both types of users must be done in person (parallel channel) avoiding incorrect identification. The user name that is traditionally used will be replaced by a RFID user ID, being that the user RFID tag is also delivered in person. Once this protocol is designed to be used in mobile applications, this will make user authentication easier for the user (of course, only when complemented by other means; the simple possession of the tag will not entitle its carrier the user identification).

For the UA the CA will only issue an user password and a RFID tag with an user ID. The password must be given to the user in a closed envelope. This password can be changed later in the client application, after strong authentication. The CA must store in the database a hash made from the user password. It is chosen to store only the password hash to protect the real password, the password hash gives only access to the access with UA. Anyone that enters the system in read-only mode won't be able to access operations as a Secure User Authentication (SUA) would, nor accessing offline files, as described in section III-C3.

For sure, an authentication scheme based on login and password is not a very secure method. Thus, it is proposed that, just like the SSL protocol, the CA also issues Public Key Certificates for each user needing Secure User Authentication, SUA. In this case the CA will issue for each user a password (in a sealed envelope), a RFID tag and a Public Key Certificate. The certificate must have a very well-defined expiration date. The CA will cipher the generated private keys with a symmetric key. This key is obtained from a hash with the input made from from the n-tuple `<user password, user ID>`. The public keys and the ciphered secret keys may be delivered to the user using a smart card. This smart cart may be a simple memory card as this won't need any computation.

The password given to the user may be changed by the client application. The user inserts his password and the application can read his ID from the tag, so the application can decipher the secret keys. If the user inserts another password, the application can cipher the secret keys with the new password.

2) User Authentication: To achieve simple user authentication a more relaxed method is proposed - a simple login and password method - and will be identified as M-Health User Authentication (cf Fig. 4), MHUA.

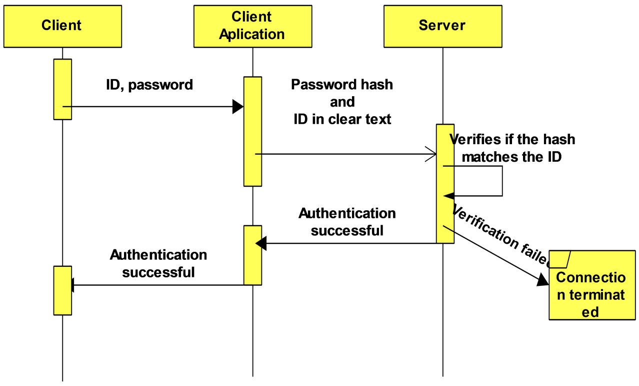
Client
Client Aplication
Server
ID, password
Password hash and ID in clear text
Verifies if the hash matches the ID
Authentication successful
Verification failed
Authentication successful
Connection terminated

Fig. 4. M-Health User Authentication (MHUA)

In this simple case, the application reads the user ID from his RFID tag and asks the user for his password. The client application will then create an hash made from the user password and send it to the server. The server will then just verify if the hash received matches the one in the database for that user. This method is easy to use and, although it is not as secure as the method in section III-C3, it provides a good level of security, because this exchange is carried out over the secure channel created by the MHSP.

3) Secure User Authentication: For a Secure User Authentication, SUA, it is necessary keeping in mind that one successful attack may lead to privileges that enable one to change a patient prescription and, eventually, putting his life in danger. So, it is necessary to design a strong authentication protocol.

The authentication protocol M-Health Secure User Authentication (MHSUA)(Fig. 5) proposed in this paper is based in Public Key Certificates. As mentioned in the registration (III-C1) phase, each user must have a password, a RFID tag, and a physical support - for instance a Smart Card[1] - with the public key certificate and the secret keys ciphered with the password. In this protocol there won't be any secret information (such as the password) exchanged using the network.

Following is the protocol in detail. The assumptions taken above in the MHSP protocol are taken in account. we also assume that $pass$ is the user password and $TagID$ is the user ID from the tag. Also UC is the user certificate and U_{pubKey} and $U_{privKey}$ are the user public and private keys. Finally $enc_{private}$ is the ciphered private key stored in the smart card, $a||b$ is the concatenation between a and b and $hash(m)$ is the hash from the input m.

1) First, the client application must read the $TagID$
2) The user selects the SUA authentication method and the application will ask for the smart card.
3) After reading the UC and the corresponding private key from the smart card the application will ask for the $pass$.
4) The client application will then get the private keys using the password.

$$U_{privKey} = dec(enc_{private}, hash(pass||Tag_ID))$$
$$CA \rightarrow S : UC$$

5) The server will then verify the authenticity of the UC and then generate a challenge to test client's authenticity.

```
if $UC$ is valid
   then Connection terminated
else $m_1 = enc(R1, U_{pubKey})$
     $S \rightarrow CApp : m_1$
```

6) To prove his authenticity the client application must be able to decipher the message m_1 using the $U_{privKey}$.

$$m_2 = dec(m_1, U_{privKey})$$
$$CApp \rightarrow S : m_2$$

7) If the received message is equal to the random data generated, the user authentication will be verified.

```
if $m_2 = r_1$
   then User authenticated
else Connection terminated
```

In the protocol above, the last message exchanged between the client and the server applications, does not need to be ciphered once the channel is already secure with the MSHP protocol.

[1] Storing the certificate and the private keys in a smart card is not mandatory. They can be stored in any keystore or support because even if an attacker gets access to them he won't be able to access the system since he hasn't the user password to decipher the secret keys.

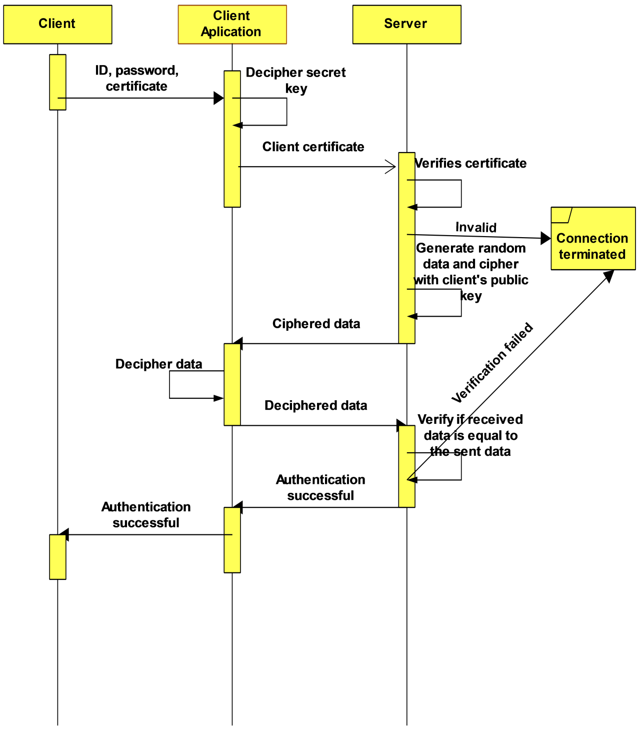
Client
Client Aplication
Server
ID, password, certificate
Decipher secret key
Client certificate
Verifies certificate
Invalid
Connection terminated
Generate random data and cipher with client's public key
Ciphered data
Decipher data
Deciphered data
Verification failed
Verify if received data is equal to the sent data
Authentication successful
Authentication successful

Fig. 5. M-Health Secure User Authentication (MHSUA)

D. Offline User Access

The protocols described previously in this paper are not appropriated for offline operations. They the need the client application connected to the server. To overcome this restriction, the client may store/cache data (using a time-to-live parameter) in his own device, for offline access. The user must be previously authenticated, using one of the above methods before being able to access and download the data. These are basically prescriptions then stored in a secure cache, within the mobile device.

The data storage method proposed in this work, named as M-Health Offline User Access, enables an offline secure access. M-Health Offline User Access uses a symmetric key. Such key is computed using a hash from a n-tuple `<user password, tag ID, name file, file creation date>`. This method assures that every file has a different key. If a given key is broken all other files will remain secured. To ensure file security, the size of each file must be limited. The application must use its key to sign each prescription before it is ciphered, assuring the prescription's integrity and authentication. Using this method one can ensure that even if different users share the application in the same device, each one will only have access to own prescriptions.

As already stated, each prescription must have its own expiration date, trustable since it is updated from a secure, identified and authenticated connection to the server; otherwise it will be marked as unusable. Therefore, this secured caching mechanism, with its temporal constraints, provides a method enabling users to control medication intakes even if the server, or their own device, is temporarily offline. Furthermore, it will enable users to update/refresh, whenever connected, the local cache and use it later on when the device is in disconnected mode, for instance when the user moves out if Internet access.

IV. MHSP Security Analysis

The MHSP protocol and MHSUA are based in a known secure protocol so, if the chosen cipher algorithms are strong enough the MHSP is safe. One of the most important points of the proposed protocols is the keys life time. It has to be carefully defined according to the chosen ciphers.

The database is assumed to be secure and only accessed with the MSHP protocol. Otherwise, the user data will be compromised, even if the used protocols are not.

To be correctly authenticated a user must have at least the tag ID, the user password and a client application with the correct public key certificate and its private keys. If the application certificate is written in a way that it has for example: the device name and network drive mac address; an attacker that has access to the application and its certificate and private keys, will also have to change his device name and his device mac. Thus, to have UA authentication an attacker must first of all, have physical access to the user device so he can get the private key. Then read the user tag ID and finally he has to find out the user password making the UA access from an attacker almost infeasible, mainly in a large scale.

The MHSUA has more security than MHUA, so it is even harder to an attacker break in. To do this, an attacker must also have the user public key certificate and its private keys.

To just sniff the data exchanged between applications, a possible attacker needs to have the application private key. To do this, the attacker needs to have physical access to the user device and this will only work for a limited time, whereas that when the certificate validity ends there must be generated a new public key for the client.

In conclusion it is possible to attack the proposed protocols and authentication methods, but they require physical access to the user devices. The proposed MHSP protocol may be vulnerable by Denial of Service (DoS) attacks, but as the proposed protocol is meant to prescriptions consultation mainly in ambulatory scenarios, if a user cant access a prescription for a few minutes it does not present any major risks.

V. Conclusion

This paper presents a set of basic security m-health mechanisms, easily deployable on mobile platforms, which would allow medication control, supported by RFID technology in Internet of Things context. Apart from managing the whole cycle, from physicians prescription to patient intake and alarms, this architecture also keeps a secure and auditable log record of all significant events and interactions with the patient's ePHR, so that any health caregiver may be implied in the process, even if the patient is at home. A pharmacist cannot repudiate that the physicians' prescription was delivered. Any nurse or other caregiver cannot repudiate to have dispensed a given medicine, at a given time, in the presence of a given patient. All this for the best of the patient's interest. Although one makes use of Internet of Things and, probably public, Internet connections, the whole system is secured, even at application level.

A new secure application layer protocol, identified as M-Health Security Protocol (MHSP), has been presented and its properties described. M-Health Security Protocol provides an application level secure channel for (mobile) client-server interactions, allowing strong authentication from both users and mobile devices. The use of RFID tags to identify entities, combined with an RFID Grouping Protocol, and with the M-Health Security Protocol, provide a complete and common security framework to implement Mobile E-Health Applications for Medication Control.

Current developments are now focused on the implementation of this security framework into the prototype for the mobile application for medication control. This work is in line with e-health service architecture and components already developed within the same project, such as the resolution of the Electronic Product Code using a versatile Object Name Service

Acknowledgment

This work is partially funded by FEDER Funds through the Programa Operacional Fatores de Competitividade - COMPETE and by National Funds through the FCT - Fundação para a Ciência e a Tecnologia (Portuguese Foundation for Science and Technology) within project FCOMP-01-0124-FEDER-022674.

References

[1] S. Meredith, P. H. Feldman, D. Frey, K. Hall, K. Arnold, N. J. Brown, and W. A. Ray, "Possible medication errors in home healthcare patients," *Journal of the American Geriatrics Society*, vol. 49, no. 6, pp. 719–724, 2001. [Online]. Available: http://dx.doi.org/10.1046/j.1532-5415.2001.49147.x

[2] M. A. P. Henriques, "Adesao ao regime medicamentoso em idosos na comunidade: eficacia das intervencoes de enfermagem (in portuguese)," Ph.D. dissertation, Universidade de Lisboa, 2011, available at http://hdl.handle.net/10451/3801.

[3] M. Sharma and A. Siddiqui, "Rfid based mobiles: Next generation applications," in *Information Management and Engineering (ICIME), 2010 The 2nd IEEE International Conference on*, april 2010, pp. 523 –526.

[4] J. Ziegler and L. Urbas, "Advanced interaction metaphors for rfid-tagged physical artefacts," in *RFID-Technologies and Applications (RFID-TA), 2011 IEEE International Conference on*, sept. 2011, pp. 73 –80.

[5] S.-L. Chen, K.-H. Lin, and R. Mittra, "A measurement technique for verifying the match condition of assembled rfid tags," *Instrumentation and Measurement, IEEE Transactions on*, vol. 59, no. 8, pp. 2123 – 2133, aug. 2010.

[6] L. Tan and N. Wang, "Future Internet: The Internet of Things," in *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*, vol. 5, aug. 2010, pp. V5–376 –V5–380.

[7] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of internet of things," in *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*, vol. 5, aug. 2010, pp. V5–484 –V5–487.

[8] I. Laranjo, J. Macedo, and A. Santos, "Internet of things for medication control: Service implementation and testing," *Procedia Technology*, vol. 5, pp. 777 – 786, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2212017312005178

[9] D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," *Wireless Personal Communications*, vol. 58, no. 1, pp. 49–69, 2011. [Online]. Available: http://dx.doi.org/10.1007/s11277-011-0288-5

[10] A. Dohr, R. Modre-Opsrian, M. Drobics, D. Hayn, and G. Schreier, "The Internet of Things for Ambient Assisted Living," in *Information Technology: New Generations (ITNG), 2010 Seventh International Conference on*, april 2010, pp. 804 –809.

[11] C.-L. Lai, S.-W. Chien, L.-H. Chang, S.-C. Chen, and K. Fang, "Enhancing medication safety and healthcare for inpatients using rfid," in *Management of Engineering and Technology, Portland International Center for*, aug. 2007, pp. 2783 –2790.

[12] C. Lee, J. Orszulak, R. Myrick, J. Coughlin, O. de Weck, and D. Asai, "Integration of medication monitoring and communication technologies in designing a usability-enhanced home solution for older adults," in *ICT Convergence (ICTC), 2011 International Conference on*, sept. 2011, pp. 390 –395.

[13] C. McCall, B. Maynes, C. Zou, and N. Zhang, "RMAIS: Rfid-based medication adherence intelligence system," in *Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE*, 31 2010-sept. 4 2010, pp. 3768 –3771.

[14] EPCglobal Inc, "Epcglobal tag data standards version 1.3.1 epcglobal ratified 552 standard," 2007, available at http://www.epcglobalinc.org/standards/tds (Online, 07/05/2013).

[15] M. Mealling, "A uniform resource name namespace for the epcglobal electronic product code (epc) and related standards," 2008, available at http://tools.ietf.org/search/rfc5134 (Online, 07/05/2013).

[16] EPCglobal Inc., "Gs1 object name service (ons) version 2.0.1," 2013, available at http://www.gs1.org/gsmp/kc/epcglobal/ons/ons_2_0_1-standard-20130131.pdf (Online, 07/05/2013).

[17] R. Sulaiman, D. Sharma, W. Ma, and D. Tran, "A security architecture for e-health services," in *Advanced Communication Technology, 2008. ICACT 2008. 10th International Conference on*, vol. 2, 2008, pp. 999–1004.

[18] M. Blaze, J. Ioannidis, and A. Keromytis, "Trust management and network layer security protocols," in *Security Protocols*, ser. Lecture Notes in Computer Science, B. Christianson, B. Crispo, J. Malcolm, and M. Roe, Eds. Springer Berlin Heidelberg, 2000, vol. 1796, pp. 103–108. [Online]. Available: http://dx.doi.org/10.1007/10720107_16

[19] M. S. Bhiogade, "Secure socket layer," June 2002. [Online]. Available: http://dx.doi.org/10.2139/ssrn.291499

[20] T. Dierks and E. Rescorl, "The transport layer security (TLS) protocol version 1.2," RFC 5246 (Proposed standard), August 2008. [Online]. Available: http://tools.ietf.org/html/rfc5246

[21] EPCglobal Inc, "Epc radio-frequency identity protocols - class-1 generation-2 uhf rfid protocol for communications at 860 mhz - 960 mhz version 1.2.0," 2008, available at http://www.gs1.org/gsmp/kc/epcglobal/uhfc1g2/uhfc1g2_1_2_0-standard-20080511.pdf (Online, 07/05/2013).

[22] P. Peris-Lopez, A. Orfila, A. Mitrokotsa, and J. C. van der Lubbe, "A comprehensive rfid solution to enhance inpatient medication safety," *International Journal of Medical Informatics*, vol. 80, pp. 13 – 24, 2011.

[23] L. C. Hadda Ben Elhadj, Nourchene Bradai and L. Kamoun, "A survey of security proposals and issues in wireless body area networks for healthcare applications," in *2012 International Conference on Software, Telecommunications and Computer Networks, SoftCOM 2012*, 2012.

[24] A. O. Pedro Peris-Lopez, J. C. Hernandez-Castro, and J. C. van der Lubbe, "Flaws on RFID grouping-proofs. guidelines for future sound protocols," *Journal of Network and Computer Applications*, vol. 34, no. 3, pp. 833 – 845, 2011, ¡ce:title¿RFID Technology, Systems, and Applications¡/ce:title¿. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804510000822

[25] P. Peris-Lopez, J. Hernandez-Castro, J. Tapiador, E. Palomar, and J. C. A. van der Lubbe, "Cryptographic puzzles and distance-bounding protocols: Practical tools for rfid security," in *RFID, 2010 IEEE International Conference on*, 2010, pp. 45–52.

[26] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2003.

[27] D. E. Robling Denning, *Cryptography and data security*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1982.

[28] HiMSS, "HIMSS Electronic Personal Health Record Definition Fact Sheet," February 2008, available at http://www.himss.org/files/HIMSSorg/content/files/ePHRdefinition_factsheet_prem.pdf (Online, 07/05/2013).