# Security Architecture for Mobile E-Health Applications in Medication Control (Arquitectura de Seguridad para Aplicaciones Móviles de Salud Electrónica en el Control de Medicamentos)

**Abstracto:**

El uso de la tecnología de identificación por radiofrecuencia (RFID) en el contexto médico permite no solo la identificación de medicamentos, sino también una identificación rápida y precisa de pacientes, médicos, enfermeras o cualquier otro proveedor de atención médica. La combinación de identificación de etiquetas RFID con soluciones de Internet de las cosas (IoT) estructuradas y seguras permite un acceso ubicuo y fácil a los registros médicos relacionados, al tiempo que proporciona control y seguridad a todas las interacciones. Este documento define una arquitectura de seguridad básica, fácilmente implementable en plataformas móviles, que permitiría establecer y administrar un servicio de prescripción de medicamentos en un contexto de movilidad utilizando registros electrónicos de salud personales. Esta arquitectura de seguridad está diseñada para ser utilizada con una aplicación móvil de salud electrónica (m-health) a través de una interfaz simple e intuitiva, compatible con la tecnología RFID. Esta arquitectura, capaz de admitir interacciones seguras y autenticadas, permitirá una fácil implementación de aplicaciones de m-health. Se presenta el caso especial de la administración de drogas y el sistema de control de medicamentos ubicuo, junto con el contexto correspondiente de Internet de las cosas. La arquitectura de seguridad y sus protocolos, junto con un servicio seguro de vida asistida general para el control de medicamentos, se analizan en el contexto de Internet de las cosas.

**Publicado en:**[2013 XXI Conferencia Internacional sobre Software, Telecomunicaciones y Redes de Computadores - (SoftCOM 2013)](https://ieeexplore.ieee.org/xpl/conhome/6657883/proceeding)

**Fecha de la conferencia:** 18-20 de septiembre de 2013

**Fecha añadida a IEEE *Xplore* :** 21 de noviembre de 2013

**ISBN electrónico:**978-953-290-040-8

**Número de acceso de INSPEC:** 13917338

**DOI:**[10.1109 / SoftCOM.2013.6671901](https://doi.org/10.1109/SoftCOM.2013.6671901)

**Editorial:**IEEE

**Lugar de la conferencia:** Primosten, Croacia

**SECCIÓN I.**

## **Introducción**

Un problema que enfrentan los servicios de salud en Portugal, y también en muchos otros países, se relaciona con sus crecientes costos, especialmente cuando se trata de asistencia especializada en centros de salud y hospitales. Como consecuencia de los altos costos de la atención médica, siempre que sea posible, muchos servicios de salud se trasladan de los hospitales a la casa del paciente. Para garantizar que no se pierda la calidad de los servicios de salud, se deben utilizar herramientas automatizadas y semiautomatizadas.

Desde el momento en que el médico prescribe el medicamento, hasta que se administra al paciente, pueden ocurrir muchos errores. Esto puede ocurrir debido a una mala interpretación de la comunicación (ya sea escrita u oral) [1] o por errores cometidos por los propios pacientes al tomar los medicamentos. El paciente debe tomar la dosis correcta del medicamento correcto en el momento correcto y esto puede controlarse mediante un acceso seguro al Registro de salud personal (PHR) del paciente.

En la clínica ambulatoria, la mayoría de las personas toman el medicamento sin asistencia médica u otra asistencia especializada, lo que aumenta la probabilidad de que ocurran errores, principalmente con pacientes de edad avanzada [2]. Para ayudar a este proceso de ingesta de medicamentos, varias tecnologías existentes pueden ayudar, siempre que se puedan minimizar los riesgos de seguridad asociados. Mediante el uso generalizado de Internet, se puede acceder a la información desde cualquier lugar; Al utilizar la identificación automática de todos los participantes, los procesos pueden ser (semi) automatizados y el error puede reducirse considerablemente. Sin lugar a dudas, pueden surgir riesgos financieros graves y de vida cuando se compromete la seguridad. Por lo tanto, la mayoría de las aplicaciones relacionadas con la salud electrónica deben aplicar procedimientos de seguridad sólidos para evitar tratamientos incorrectos, identificaciones erróneas o acceso no autorizado. Además, debe existir un registro de todos los eventos significativos, de modo que se pueda detectar cualquier negligencia del cuidador de salud.

La identificación de radiofrecuencia, comúnmente conocida como RFID, se utiliza en muchas aplicaciones [3] , [4] . El uso de esta tecnología está en constante evolución y se está expandiendo a un ritmo exponencial. Existen varios métodos de identificación, aunque el más común es un microchip capaz de almacenar un número de serie que identifica a la persona, objeto u objeto. Utilizando dispositivos electrónicos que emiten señales de radiofrecuencia, es posible realizar una captura automática de datos (en este contexto llamada etiqueta [5] ), desde un lector. Por lo tanto, RFID es una tecnología de información de adquisición que permite la autoidentificación.

El uso de Internet para transportar información contenida en etiquetas se conoce comúnmente como " *Internet de las cosas* " [6] , [7] . Este término se define como objetos con identidad y personalidad virtual que, mientras trabajan en espacios inteligentes, utilizan interfaces para conectarse y comunicarse en un contexto social, ambiental y personal.

Este trabajo analiza y presenta nuevos protocolos y soluciones de seguridad para integrarse en la arquitectura de servicios de salud móvil [8] , donde se propone un sistema de control remoto de medicamentos para la vida asistida ambiental, especialmente dirigido a personas mayores.

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] 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])

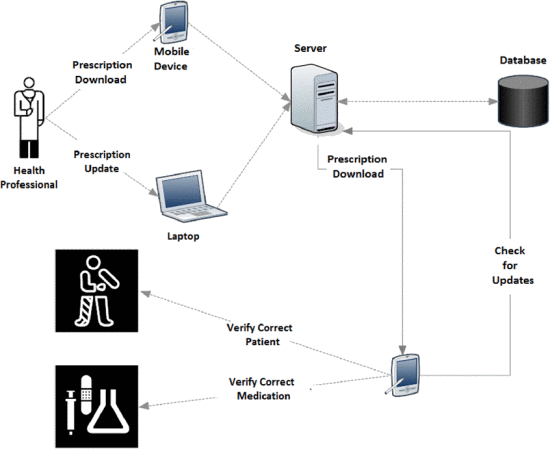
Como se puede observar en la Tabla I , una gran mayoría de los ancianos necesita ayuda en el control de medicamentos, ya que el 82.8% señala las razones por las cuales los sistemas AAL semiautomáticos pueden ser de gran ayuda.

### B. Escenario de aplicación de M-Health

En [8], se propone un Servicio de e-Health, cuyo objetivo principal es desarrollar un servicio de m-health simple para AAL, basado en tecnologías RFID e IoT. El objetivo principal del marco de seguridad presentado en este documento es el establecimiento de una arquitectura segura y control de acceso al sistema de información que relaciona pacientes, recetas y medicamentos, para verificar fácilmente, especialmente en movilidad, el cumplimiento por parte de los pacientes de lo prescrito. medicamentos y dosis. Este servicio de m-health para AAL supone que los médicos, pacientes y medicamentos deben identificarse mediante etiquetas RFID y que todo el proceso, desde la prescripción hasta la administración de medicamentos farmacéuticos, debe controlarse mediante un sistema de información basado en IoT . Todo el proceso comienza en un centro de salud cuando el médico prescribe un conjunto de medicamentos farmacéuticos al paciente, identificándose tanto el médico como el paciente mediante etiquetas RFID. Estas etiquetas permiten el establecimiento de una arquitectura IoT y mecanismos de control de acceso al sistema de información que relaciona pacientes, recetas y medicamentos.

Se supone que los médicos completan la receta donde incluyen la dosis y el tiempo en que se tomará el medicamento. Esta información se almacena en la base de datos del sistema de salud electrónica, ya vinculada a la etiqueta RFID asignada a cada paciente. Estas etiquetas pueden leerse mediante lectores RFID ubicados en cualquier hardware específico, pero también (y especialmente) mediante lectores conectados a dispositivos móviles de uso general, como teléfonos inteligentes, tabletas, PDA, etc.

En dicho contexto, como se muestra en la Figura 1 , el paciente tendrá un teléfono inteligente (o una tableta) con la aplicación m-health. Los médicos, utilizando sus propios dispositivos personales o institucionales (móviles o fijos) emitirán recetas que se actualizarán inmediatamente en la base de datos. El dispositivo móvil de los pacientes accederá a esa base de datos y actualizará las recomendaciones médicas que se pueden descargar para utilizarlas en modo fuera de línea. Los dispositivos móviles, que utilizan la tecnología RFID, permiten a los farmacéuticos entregar la medicación correcta a los usuarios y a los usuarios verificar que toman la medicación correcta en el momento adecuado. A lo largo de todo este proceso, la seguridad es una preocupación importante: se debe garantizar la confidencialidad e integridad de los datos, se debe verificar la autenticación de los usuarios e incluso de las aplicaciones.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/6657883/6671843/6671901/6671901-fig-1-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/6657883/6671843/6671901/6671901-fig-1-source-large.gif)

**Figura 1.**M-Health Application Scenario

[View All](https://ieeexplore.ieee.org/document/6671901/all-figures)

**SECTION 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 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.

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

[View All](https://ieeexplore.ieee.org/document/6671901/all-figures)

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 in advance. 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

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 and that no revocation occurred. 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).

**SECTION 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].

En un entorno de salud, el sistema es importante para equilibrar la seguridad del sistema con la disponibilidad. Un acceso no autorizado puede ser perjudicial para el sistema o los pacientes, pero en caso de emergencia si el personal médico no puede alcanzar la información necesaria, puede ser aún más peligroso, principalmente para los pacientes. Teniendo esto en cuenta, proponemos la creación de dos tipos de acceso: uno con permiso de solo lectura y otro con permiso de lectura y escritura. En este esquema, la seguridad puede ser un poco más relajada en el acceso de solo lectura, haciendo que la información esté más fácilmente disponible. En el acceso de lectura y escritura, la seguridad es más estricta porque agregar o modificar información importante puede ser catastrófico, ya sea financieramente o incluso para la vida de los pacientes.

Se supone que toda la información del paciente a la que se debe acceder es manejable en el contexto del Registro de Salud Personal (ePHR) electrónico del paciente. Según la definición de la *Sociedad de Sistemas de Información y Gestión* de la *Atención Médica,* un Registro electrónico de salud personal (ePHR) [28] es un "[ ... ] *herramienta de por vida para gestionar la información de salud relevante, promover el mantenimiento de la salud y ayudar con el manejo de enfermedades crónicas a través de un conjunto interactivo de datos comunes de información de salud electrónica y herramientas de salud electrónica* .[ ... ] El ePHR es propiedad, administrado y compartido por la persona o sus apoderados legales y debe ser seguro para proteger la privacidad y confidencialidad de la información de salud que contiene ".

Los profesionales de la salud y los pacientes deben acceder al sistema de TI que admite el ePHR del paciente. Los pacientes recibirán un dispositivo móvil desde donde accederán al sistema y su ePHR. Los profesionales de la salud podrán acceder al sistema con un dispositivo móvil o una computadora portátil.

Se permitirá un acceso de solo lectura con el dispositivo conectado o desconectado a Internet, pero el acceso de lectura y escritura siempre requerirá una conexión a Internet debido al protocolo de autenticación (fuerte) propuesto en este documento. Todos los accesos al ePHR deben ser auditables, manteniendo un registro robusto que identifique claramente al usuario, el momento de ocurrencia y la operación de datos asociada realizada.

Además, todas las comunicaciones entre las etiquetas RFID y los lectores utilizarán un protocolo seguro, como el Protocolo de agrupación propuesto por [22] o los acertijos criptográficos propuestos por [25] . El protocolo propuesto por [22] debería ser más apropiado para aplicar en este caso, una vez que ofrezca una forma de establecer la asociación entre la medicación-prescripción-paciente y la autenticación. Ofrece un buen nivel de seguridad, siempre que el PIN de la etiqueta tenga suficiente entropía [22] , y sea fácil de implementar.

Para fines de autenticación, el protocolo propuesto por [25] también es adecuado. También tiene un buen nivel de seguridad, pero es más difícil de implementar. Peris-Lopez y col. [25] tiene un nuevo enfoque para la seguridad RFID: las etiquetas generan un rompecabezas para que el lector lo resuelva, haciendo uso de un protocolo de límite de tiempo que aumenta la dificultad del rompecabezas con el aumento de la distancia del lector de etiquetas.

### B. Protocolo de seguridad de M-Health

Se propone y presenta dentro de esta sección un nuevo protocolo de seguridad dirigido a aplicaciones móviles de salud electrónica, identificado como M-Health Security Protocol (MHSP). El protocolo propuesto (cf. Fig. 3 ) encuentra sus raíces en el conocido protocolo SSL. En lugar de usarlo en la capa de transporte tradicional, MHSP estaba dirigido a la capa de aplicación. Esta elección se realizó debido a la gran seguridad proporcionada, notando también que SSL es ampliamente utilizado en Internet global.

Este protocolo proporciona un canal seguro a través de Internet y la autenticación entre las aplicaciones. La autenticación entre aplicaciones se logra mediante certificados de clave pública. Este certificado puede ser verificado por una Autoridad de certificación (CA).

Following, the proposed MHSP protocol will be explained in detail. It 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 mn 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. SpubKey and SprivKey are the server's public and private key, the same happens with CApppubKey and CAppprivKey, 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→S:CC

View Source

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

[View All](https://ieeexplore.ieee.org/document/6671901/all-figures)

1. The Server Application verifies the validity of the received certificate, terminating the connection if not verified.
2. 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.
3. In this phase the server will have to prove its authenticity to the client using the challenge received. Then it will generate the session and communications keys.
4. With the reply the client application can verify the server's authenticity and obtain the session and communications keys
5. Finally the server will decipher the message m4 sent by the client application and, if deciphered correctly, it means that the client application was able to decipher the Commkey correctly and the client is authenticated.

Previously two symmetric keys were mentioned: 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, two possible scenarios were proposed: one for prescription writing (read-write operations) and another one for prescription consultation (read-only operations); these scenarios will be identified as 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).

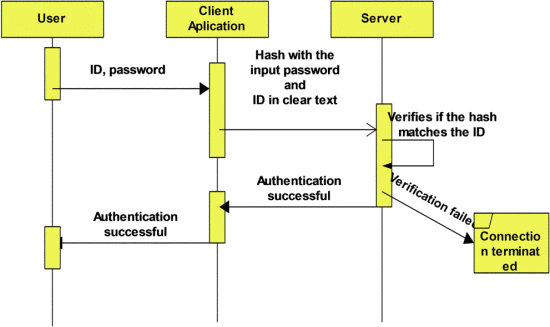
For the UA the CA will only issue an user password and a RFID tag with an user ID. The password must be given to the user in a closed envelope. This password can be changed later in the client application, after strong authentication. The CA must store in the database a hash made from the user password. 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.

Por supuesto, un esquema de autenticación basado en inicio de sesión y contraseña no es un método muy seguro. Por lo tanto, se propone que, al igual que el protocolo SSL, la CA también emite certificados de clave pública para cada usuario que necesite autenticación de usuario segura, SUA. En este caso, la CA emitirá para cada usuario una contraseña (en un sobre cerrado), una etiqueta RFID y un Certificado de clave pública. El certificado debe tener una fecha de vencimiento muy bien definida. La CA cifrará las claves privadas generadas con una clave simétrica. Esta clave se obtiene de un hash con la entrada realizada desde la n-tupla <contraseña de usuario, ID de usuario>. Las claves públicas y las claves secretas cifradas se pueden entregar al usuario utilizando una tarjeta inteligente. Este carrito inteligente puede ser una simple tarjeta de memoria, ya que no necesitará ningún cálculo.

La aplicación del cliente puede cambiar la contraseña dada al usuario. El usuario inserta su contraseña y la aplicación puede leer su ID de la etiqueta, por lo que la aplicación puede descifrar las claves secretas. Si el usuario inserta otra contraseña, la aplicación puede cifrar las claves secretas con la nueva contraseña.

#### 2) Autenticación de usuario

Para lograr una autenticación de usuario simple, se propone un método más relajado, un método simple de inicio de sesión y contraseña, que se identificará como Autenticación de usuario de M-Health (ver Fig. 4 ), MHUA.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/6657883/6671843/6671901/6671901-fig-4-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/6657883/6671843/6671901/6671901-fig-4-source-large.gif)

**Fig.4.**Autenticación de usuario de M-Health (MHUA)

[Ver todo](https://ieeexplore.ieee.org/document/6671901/all-figures)

En este caso simple, la aplicación lee la identificación de usuario de su etiqueta RFID y le pide al usuario su contraseña. La aplicación cliente creará un hash creado a partir de la contraseña del usuario y lo enviará al servidor. El servidor solo verificará si el hash recibido coincide con el de la base de datos para ese usuario. Este método es fácil de usar y, aunque no es tan seguro como el método en la sección III-C3 , proporciona un buen nivel de seguridad, ya que este intercambio se realiza a través del canal seguro creado por el MHSP.

#### 3) Autenticación segura del usuario

Para una Autenticación segura de usuario, SUA, es necesario tener en cuenta que un ataque exitoso puede generar privilegios que le permitan cambiar la prescripción de un paciente y, finalmente, poner en peligro su vida. Por lo tanto, es necesario diseñar un protocolo de autenticación fuerte.

El protocolo de autenticación M-Health Secure User Authentication (MHSUA, Fig. 5 ) propuesto en este documento se basa en certificados de clave pública. Como se mencionó en la fase de registro (III-C1), cada usuario debe tener una contraseña, una etiqueta RFID y un soporte físico, por ejemplo, una tarjeta inteligente 1 , con el certificado de clave pública y las claves secretas cifradas con la contraseña. En este protocolo no se intercambiará información secreta (como la contraseña) utilizando la red.

Detailed protocol description follows. The assumptions above, for the MHSP protocol, are again considered; it is also assumed that *pass* is the user password and TagID is the user ID retrieved from the tag. Also UC is the user certificate and UpubKey and UprivKey are the user public and private keys. Finally encprivate 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.

UprivKey=dec(encprivate,hash(pass∥TagID))CA → S: UC

Ver fuente

1. El servidor verificará la autenticidad del UC y luego generar un desafío para probar la autenticidad del cliente.
2. Para demostrar su autenticidad, la aplicación del cliente debe poder descifrar el mensaje metro1 utilizando el Up r i v Ke y.

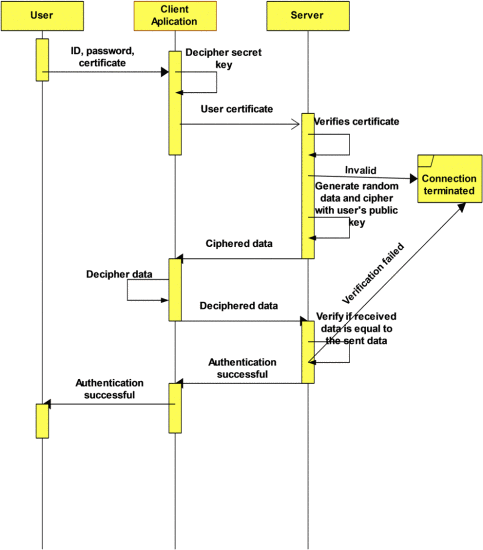
metro2= de c ( m1, Up r i v Ke y)CA p p → S: m2

Ver fuenteRight-click on figure for MathML and additional features.

1. Si el mensaje recibido es igual a los datos aleatorios generados, se verificará la autenticación del usuario.

[[Algorithm ](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/6657883/6671843/6671901/6671901-alg-7-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/6657883/6671843/6671901/6671901-alg-7-source-large.gif)

En el protocolo anterior, no es necesario cifrar el último mensaje intercambiado entre el cliente y las aplicaciones del servidor, ya que el canal ya está seguro con el protocolo MSHP.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/6657883/6671843/6671901/6671901-fig-5-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/6657883/6671843/6671901/6671901-fig-5-source-large.gif)

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

[View All](https://ieeexplore.ieee.org/document/6671901/all-figures)

### D. Offline User Access

The protocols described previously in this paper are not appropriated for offline operations. They 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.

Como ya se indicó, cada receta debe tener su propia fecha de vencimiento, confiable ya que se actualiza desde una conexión segura, identificada y autenticada al servidor; de lo contrario, se marcará como inutilizable. Por lo tanto, este mecanismo de almacenamiento en caché seguro, con sus limitaciones temporales, proporciona un método que permite a los usuarios controlar la ingesta de medicamentos incluso si el servidor o su propio dispositivo está temporalmente fuera de línea. Además, permitirá a los usuarios actualizar / actualizar, siempre que esté conectado, el caché local y usarlo más tarde cuando el dispositivo esté en modo desconectado, por ejemplo, cuando el usuario se mude si tiene acceso a Internet.

**SECCION IV.**

## **Análisis de seguridad de MHSP**

El protocolo MHSP y MHSUA se basan en un protocolo seguro conocido, por lo que el MHSP es seguro, siempre que los algoritmos de cifrado sean lo suficientemente fuertes. Una de las cuestiones más importantes de los protocolos propuestos es la duración de las claves, por lo que la duración de la clave debe definirse cuidadosamente de acuerdo con los cifrados elegidos. Se supone que la base de datos física es segura y solo se accede con el protocolo MSHP. De lo contrario, se puede acceder a los datos sin procesar del usuario, incluso si los protocolos de seguridad no se ven comprometidos.

Para poder autenticarse, un usuario debe tener al menos el ID de la etiqueta, debe conocer la contraseña del usuario y tener una aplicación cliente con la clave pública correcta y sus claves privadas. Los atributos del certificado de la aplicación deben incluir la identificación del dispositivo y la dirección MAC de la unidad de red; un atacante que tenga acceso a la aplicación, su certificado y clave privada, también tendrá que cambiar su propia identificación del dispositivo y el dispositivo MAC correspondiente. Por lo tanto, para tener éxito en la autenticación UA, un atacante debe, antes que nada, tener acceso físico al dispositivo del usuario para que pueda obtener la clave privada; el atacante también debe conocer la identificación de la etiqueta del usuario y finalmente descubrir la contraseña del usuario. El acceso a la combinación única correcta de todos estos elementos hace que la personificación de la AU sea casi inviable, principalmente a gran escala.

El MHSUA es aún más seguro que MHUA, por lo que es aún más difícil para un atacante entrar. Para tener éxito, un atacante también debe poder acceder y descifrar el certificado de usuario y acceder a su clave privada. Para poder rastrear los datos intercambiados entre aplicaciones, un atacante potencial necesita conocer la clave privada de la aplicación. Para hacer esto, el atacante necesita tener acceso físico al dispositivo del usuario, para extraer y descifrar los datos almacenados localmente. Incluso entonces, esto compromete solo un período de tiempo limitado, hasta revocar el certificado del cliente, invalidando sus claves.

En conclusión, aunque no es imposible atacar los protocolos y métodos de autenticación propuestos, esto requiere el conocimiento de varios datos privados del usuario y acceso físico al dispositivo del usuario. Finalmente, el protocolo MHSP puede estar expuesto a ataques de denegación de servicio (DoS), pero esto no compromete ningún dato (el usuario no puede leer las recetas por algún tiempo) y puede verse afectado por las protecciones de red normales.

**SECCION V.**

## **Conclusión**

Este documento presenta una arquitectura segura, un conjunto de mecanismos básicos de seguridad de salud móvil y protocolos asociados, fácilmente implementables en plataformas móviles, que permiten el control de medicamentos, con el apoyo de la tecnología RFID en el contexto de Internet de las cosas. Además de ocuparse de todo el ciclo, desde la prescripción de los médicos hasta la admisión y las alarmas del paciente, esta arquitectura también mantiene un registro de registro seguro y auditable de todos los eventos e interacciones importantes con el ePHR del paciente, de modo que cualquier cuidador de salud pueda estar implicado en el proceso, incluso si el paciente está en casa. Un farmacéutico no puede repudiar que se entregó la receta del médico; una enfermera u otro cuidador no puede repudiar haber dispensado un medicamento determinado, en un momento dado, en presencia de un paciente determinado. Todo esto para el mejor interés del paciente.

El Protocolo de seguridad M-Health (MHSP), cuyas propiedades y análisis de seguridad se presentan, proporciona un canal seguro a nivel de aplicación para las interacciones cliente-servidor (móvil), lo que permite una autenticación sólida tanto de usuarios como de dispositivos móviles. Como se discutió, el uso de etiquetas RFID para identificar entidades, combinado con un Protocolo de agrupación RFID y con el Protocolo de seguridad M-Health, proporciona un marco de seguridad completo y común para implementar aplicaciones móviles de E-Health para el control de medicamentos.

Los desarrollos actuales se centran ahora en la implementación de este marco de seguridad en el prototipo de la aplicación móvil para el control de medicamentos. Este trabajo está en línea con la arquitectura del servicio de salud electrónica y los componentes ya desarrollados dentro del mismo proyecto, como la resolución del EPC utilizando un servicio de nombres de objetos versátil.

### RECONOCIMIENTO

Este trabajo está parcialmente financiado por FEDER Funds a través del Programa Operacional Fatores de Competitividade-COMPETE y por National Funds a través de FCT - Fundação para a Ciência ea Tecnologia (Fundación portuguesa para la ciencia y la tecnología) dentro del proyecto FCOMP-01–0124-FEDER-022674 .