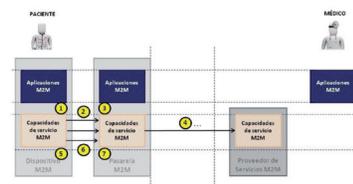


Esquemas conceptuales para arquitecturas M2M en el contexto de la e-salud.

Una revisión integral de los casos de uso y tendencias de estandarización

CONCEPTUAL SCHEMES FOR M2M ARCHITECTURES IN E-HEALTH CONTEXT.
A COMPREHENSIVE USE CASES REVIEW AND STANDARDIZATION TRENDS



DOI: <http://dx.doi.org/10.6036/7138> | Recibido: 10/04/2014 • Aceptado: 06/10/2014

Eduardo Pérez-Cebollada, Ignacio Martínez-Ruiz,
José L. Bernal-Agustín

UNIVERSIDAD DE ZARAGOZA. Dpto. Ingeniería Eléctrica. Calle
María de Luna, 3 – 50018 Zaragoza. Tlfno: +34 976 761921

ABSTRACT

• The interest in machine-to-machine (M2M) systems has grown in recent years due to ubiquitous wireless availability and declining prices of communication modules. Although in some areas this concept has developed adequately, e-Health is not one of them. The European Telecommunications Standards Institute (ETSI) has made great efforts to develop standards in this field, but the resulting documents are sometimes difficult to understand and include extensive technical information.

The first objective of this research is to place the M2M architecture defined by ETSI in the environment of e-Health, identifying theoretical concepts with real situations and specific devices. Then, our work analyses use cases of M2M applications for e-Health defined by ETSI, clarifying ambiguous situations. To review the use cases, we employ a personal and simplified scheme for the architecture that is based on a vertical and horizontal model, which allows a visual and intuitive interpretation of the steps executed in the different scenarios. The engineers will have several diagrams with interacting entities that represent a very useful aid for system design and implementation.

In the review, we also find the importance of energy efficiency in e-Health, especially in life-critical applications, which may be the subject of further investigations. On the other hand, our study reveals the main problem with medical devices: the plurality of communications protocols established by suppliers. The current ISO/IEEE 11073 standards, which enable interoperability between these devices, may be a good starting point to achieve M2M standardization in this area.

• **Keywords:** M2M, IoT, e-Health, ETSI, service capabilities, use cases, ISO/IEEE 11073.

RESUMEN

El interés de los sistemas “Máquina a Máquina” (*Machine to Machine*, M2M) ha experimentado un gran auge en los últimos años gracias a la alta disponibilidad de conexiones inalámbricas y al descenso de precios en los módulos de comunicación. Aunque en algunas áreas este concepto se ha desarrollado adecuadamente, la e-Salud no es una de ellas. El *European Telecommunications Standards Institute* (ETSI) ha hecho grandes esfuerzos en proponer estándares en este campo, pero los documentos resultantes son, en algunos casos, difíciles de comprender e incluyen excesiva información técnica.

El primer objetivo de este artículo es relacionar la arquitectura M2M y los conceptos teóricos definidos por el ETSI en el entorno de la e-Salud, con situaciones reales y dispositivos concretos. Una vez situados, en segundo lugar, se analizan los casos de uso definidos por el ETSI para las aplicaciones M2M en la e-Salud, con la intención de clarificar situaciones y términos ambiguos. Para revisar estos casos, hemos diseñado un esquema simplificado de la arquitectura, basado en un modelo vertical y horizontal, que nos permite de una manera visual e intuitiva interpretar los pasos a ejecutar en los diferentes escenarios propuestos. Los ingenieros dispondrán así de un conjunto de diagramas con entidades interactivas que representarán una ayuda muy útil para el diseño e implementación de estos sistemas.

Además, en nuestra revisión, nos encontramos con la importancia que cobra la eficiencia energética en la e-Salud, especialmente en las aplicaciones críticas para la vida, lo que puede dar lugar a posteriores investigaciones en ese sentido. Igualmente, nuestro estudio nos revela el principal problema existente en los dispositivos médicos: la pluralidad de protocolos ofrecidos por los proveedores. La actual familia de estándares ISO/IEEE 11073, que permite la interoperabilidad entre estos dispositivos, puede ser un buen punto de partida hacia la estandarización M2M en este campo.

Palabras clave: M2M, IoT, e-Salud, ETSI, capacidades de servicio, casos de uso, ISO/IEEE 11073.

1. INTRODUCCIÓN

El concepto de “Internet de las cosas” (*Internet of Things*, IoT) [1, 2], donde cualquier dispositivo o máquina adquiere la habilidad de conectarse a la red y socializar con otros, es una idea brillante, pero simple; es necesario definir una arquitec-

tura con elementos activos capaces de interactuar unos con otros usando protocolos que proporcionen una conectividad universal. Por ello, el concepto debe ser considerado dentro de una arquitectura “Máquina a Máquina” (*Machine to Machine*, M2M) que soporte la comunicación entre un grupo de dispositivos capaces de transmitir y recibir datos de manera autónoma, sin intervención humana [3].

En los últimos años, se han intentado describir los requisitos de un sistema de extremo a extremo (*end-to-end*) que soporte servicios M2M en diferentes áreas: redes eléctricas inteligentes (*smart grids*), consumo personal, automatización de ciudades, sistemas de automoción y e-Salud. Estos estándares están muy avanzados en algunas de estas áreas de interés (como en *smart grids* o en sistemas de automoción), pero en e-Salud sigue siendo un tema de interés sin demasiados antecedentes al respecto, lo que justifica este artículo.

Por otro lado, en el campo de la e-Salud, se está trabajando en el contexto internacional de normalización e interoperabilidad, impulsado principalmente desde Europa, para avanzar a todos los niveles (funcional, sintáctico, semántico, estructural, organizativo, etc.) en el intercambio de datos de salud que garanticen globalmente la continuidad asistencial. En este ámbito, hay que destacar el papel trascendente que juegan entidades como *Continuous Health Alliance*, *Personal Connected Health Alliance* (PCHHA), o *Integrating the Healthcare Enterprise* (IHE) dentro del marco de los proyectos y planes estratégicos referentes en este sector como el proyecto europeo epSOS [4], el *eHealth Action Plan 2012-2020* [5] y el *eHealth European Interoperability Framework* [6] entre otros.

En todo este contexto, el *European Telecommunications Standards Institute* (ETSI) se ha sumado para documentar aplicaciones específicas M2M en el campo de la *e-Salud* que podrían ser de interés: el control de enfermedades (ej. diabetes y arritmias cardíacas), la independencia de las personas mayores (como ayuda a la gente mayor para llevar una vida independiente) y el mantenimiento personal y mejora de la salud (en base a registros de indicadores de salud y bienestar tales como frecuencias cardíacas y respiratorias, consumo de energía y tasa de grasa quemada durante sesiones de ejercicio). En todos estos ejemplos, los datos son recogidos por uno o más sensores y enviados a un servidor *back-end*, pero la cantidad de datos y su frecuencia dependen de lo críticas que sean las condiciones de salud del paciente. Por ejemplo, en contraste

con las aplicaciones M2M relacionadas con el control de enfermedades e independencia de las personas mayores, en el mantenimiento personal y mejora de la salud, es más probable que se requiera una carga inicial de datos menor y que se sea más tolerante con los retrasos en los envíos de datos.

En este contexto de comunicaciones M2M, el ETSI ha elaborado una serie de documentos técnicos, listados en la Tabla I y disponibles en <http://pda.etsi.org>. Uno de los documentos clave es el TR 102732 referido a las descripciones de los casos de uso para aplicaciones de e-Salud, porque a partir de él podrán desarrollarse las aplicaciones M2M anteriormente citadas. Sin embargo, los diferentes escenarios descritos en estos casos de uso se explican en base a información técnica de alta complejidad, con muchas referencias a la arquitectura M2M descrita en el TS 102690 y a conceptos definidos en los otros documentos, pero sin especificarlos, lo que dificulta su comprensión.

En este artículo, después de una evaluación de los problemas concretos del M2M aplicado a la e-Salud, la Sección II aporta un esquema conceptual, muy visual, de la arquitectura M2M bajo una doble orientación: vertical y horizontal (V-H), de igual forma que la Unión Internacional de Telecomunicaciones (*International Telecommunication Union*, ITU) ha hecho con otras arquitecturas como las Redes de Nueva Generación [7], de tal manera que la red jerárquica M2M queda reflejada en sentido vertical y las diferentes entidades que la componen se muestran en sentido horizontal. Después, en la Sección III revisamos en profundidad los casos de usos de las aplicaciones M2M en la e-Salud definidos por el ETSI y los trasladamos a este esquema conceptual V-H, con el fin de proporcionar una visión más compacta y diáfana de ellos, detallando además las capacidades de servicio que se ven implicadas en la comunicación. La Sección IV aborda la estandarización M2M en el campo de la e-Salud, los problemas que entraña, y cómo el estándar ya existente para comunicación de dispositivos médicos ISO/IEEE 11073, puede ser un buen punto de partida. Finalmente, se muestran las conclusiones y se proponen futuros trabajos.

2. MATERIALES Y MÉTODOS

El principal logro de la arquitectura funcional M2M que vamos a describir, es presentar, de extremo a extremo, las entidades funcionales M2M y la relación entre estas entidades dentro de una red jerárquica. Básicamente, la arquitectura se divide en dos dominios (ver el esquema conceptual de la Fig.1). Vamos a analizarlos en detalle, respetando también sus términos en inglés para seguir la concordancia con los documentos ETSI, principalmente TS 102690 y TR 102732:

- 1) Dominio de Dispositivo y de Pasarela (*Device and Gateway Domain*, DGD), compuesto por las siguientes entidades:
 - Dispositivo M2M (*M2M Device*): un dispositivo sobre el que corren aplicaciones M2M gracias a la capa de capacidades de servicio M2M (*M2M service capabilities*).
 - Pasarela M2M (*M2M Gateway*): una pasarela (también con aplicaciones M2M y capacidades de servicio M2M) que actúa como proxy entre los dispositivos M2M y el dominio de red, en el caso de que el dispositivo M2M no

Nº Informe	Contenido
TS 102689	Requerimientos de servicio M2M
TS 102690	Arquitectura funcional M2M
TS 102921	Comunicaciones M2M; interfaces mla, dla y mld
TR 102732	Descripción de casos de uso para aplicaciones e-Salud en el contexto de comunicaciones M2M
SR 002564	Aplicabilidad de los entregables existentes de ETSI y ETSI/3GPP en e-Salud
TR 102764	Arquitectura en e-Salud; análisis de los modelos de servicio de usuario, tecnologías y aplicaciones que soportan e-Salud

Tabla I: Documentos ETSI relativos a estándares de M2M en e-Salud

- tuviera conectividad directa con el dominio de red.
- Red de Área M2M (*M2M Area Network*): red que proporciona comunicación entre los dispositivos M2M y la pasarela M2M por medio de diferentes tecnologías (ZigBee, Bluetooth, 6lowPAN, y otras). Una red local (LAN o PAN) puede formar parte de la red de área M2M.
- 2) Dominio de red (*Network Domain, ND*), que se compone de las siguientes entidades:
- Red de Acceso (*Access Network*): red que permite a los dispositivos M2M y a la pasarela M2M conectarse con la red troncal, a través de ciertas tecnologías (xDSL, HFC, WiMAX, y otras).
 - Red Troncal (*Core Network*): red que proporciona conectividad IP, interconexión con otras redes, roaming y otras funciones de red. La tecnología empleada puede ser 3GPP, ETSI TISPAN, 3GPP2, etc.
 - Capacidades de servicio M2M (*M2M Service Capabilities*): capa que proporciona un grupo de funciones M2M compartidas y accesibles por diversas aplicaciones. En este dominio, pueden residir en el proveedor de servicios M2M (*M2M service provider*), entendiendo éste como uno o más servidores back-end de la red troncal.
 - Aplicaciones M2M (*M2M Applications*): aplicaciones donde corre la lógica de servicio y que usan las capacidades de servicio, accesibles a través de interfaces abiertos.

Un aspecto importante a tener en cuenta es que cada uno de los nodos M2M de la arquitectura - los dispositivos M2M, la pasarela M2M y el proveedor de servicios M2M - poseen capacidades de servicio M2M (ver Fig.1). Es decir, estas capacidades de servicio pueden ser invocadas desde diferentes puntos del sistema. O dicho de otra forma, esta capa proporciona funciones que permiten la comunicación extremo a extremo entre aplicaciones.

El ETSI identifica un número de capacidades de servicio M2M, como las siguientes:

- Activación de aplicaciones (*Application Enablement, xAE*). Proporciona acceso a las aplicaciones.
- Comunicación genérica (*Generic Communication, xGC*). Gestiona todos los aspectos relacionados con el transporte de datos.
- Accesibilidad, direccionamiento y repositorio (*Reachability, Addressing and Repository, xRAR*). Almacena información y proporciona direcciones de red enrutables.
- Selección de comunicación (*Communication Selection, xCS*). Proporciona selección entre redes (si esto fuera posible)
- Gestión remota de entidades (*Remote Entity Management, xREM*). Posee funciones relativas a la gestión del ciclo de vida de las entidades.
- Seguridad (*Security, xSEC*). Implementa aspectos de seguridad como autenticación y gestión de claves.

Donde la x puede ser N si nos referimos a la red (proveedores de servicios), G si nos referimos a la pasarela, o D para dispositivos. Además de las citadas, en el campo de la e-Salud, las aplicaciones pueden también invocar a capacidades funcionales específicas que ayuden a facilitar las actividades de intercambio de información referentes a la salud. Uno de los objetivos de este trabajo es determinar cuáles son y en qué punto del sistema se producen estas capacidades de servicio

M2M, identificándolas en los diferentes pasos de que constan los casos de uso descritos en TR 102732.

Al igual que sucede con las capacidades de servicio, hay aplicaciones en ambos dominios (ver Fig.1). En el DGD, las aplicaciones pueden comunicarse con y/o controlar los dispositivos M2M sin salir de la red de área M2M; pero en el ND, las aplicaciones envían solicitudes a estos dispositivos M2M atravesando la red troncal. En nuestro trabajo, identificaremos también el dominio correspondiente cuando en los casos de uso se hagan referencia a las diferentes aplicaciones.

Para conseguir nuestros objetivos, la primera labor a desarrollar es trasladar la compleja y teórica arquitectura M2M definida por la ETSI para el contexto de la e-Salud, a una propuesta más didáctica de esquemas conceptuales V-H (ver Fig.1) basados en un escenario real. El DGD, habitualmente, se asocia al entorno del usuario final-paciente monitorizado (bien en el domicilio, la residencia, el hospital, etc.) al que, por facilitar la comprensión, se le asigna el término de 'Paciente'. Este paciente lleva uno o más dispositivos M2M con sensores que registran diferentes indicadores de salud o bienestar tales como la presión sanguínea, la temperatura corporal, la frecuencia cardíaca, u otros. Sin embargo, estos dispositivos tienen varias limitaciones (como el consumo de la batería o su alcance) y necesitan otro dispositivo que actúe como recolector de la información recogida y como pasarela para enviar los datos de salud al servidor back-end a través de una WAN (*Wide Area Network*), desde donde pueden ser vistos por el médico. Esta pasarela M2M puede ser un dispositivo fijo, como un ordenador personal o un *router*, o un dispositivo móvil, como un teléfono móvil o incluso un aparato autónomo colocado alrededor de la muñeca o el cuello del paciente. Sin embargo, si los dispositivos M2M tienen la capacidad de proporcionar conectividad extremo a extremo hasta el servidor *back-end* (gracias a un módulo de integración WAN) no necesitan la ayuda de la pasarela M2M.

Por otro lado, el ND, habitualmente, se asocia al entorno del usuario final-coordinador de salud al que, por facilitar la comprensión, se le asigna el término de 'Médico' e incluye tanto a personas físicas como a aplicaciones bajo la supervisión médica que puedan evaluar la información recibida desde los dispositivos M2M del paciente y determinar cuál es la intervención clínica adecuada a llevar a cabo. Estos coordinadores usan un terminal (que puede ser un aparato electrónico como un *smartphone*, una agenda digital, un ordenador personal, o similar) con una aplicación M2M instalada en ellos. El coordinador puede conectar con el servidor back-end a través de la ejecución de la aplicación M2M correspondiente.

Cabe destacar, que éste es el escenario habitual, aunque pueden existir otro tipo de usuarios en cada uno de los dos dominios especificados ya que, por ejemplo, puede haber aplicaciones M2M en dispositivos M2M destinadas al personal sanitario (como una aplicación en el móvil de un profesional sanitario que fuera capaz de "decidir" si alertar o no al médico). En estos casos, aunque el rol de 'Medico' estaría asociado al DGD, la propuesta planteada de esquemas V-H sigue siendo válida en términos generales, ajustando esta asignaciones de roles y permitiendo reflejar que las aplicaciones M2M del lado de los profesionales pueden residir en dispositivos M2M.

Con todas estas consideraciones, una de las contribuciones consistirá en una revisión de los casos de uso más importantes

descritos en TR 102732, agrupando y simplificando el mapeo funcional y los pasos a ejecutar en otros más precisos que se describirán en las correspondientes tablas y figuras a partir del esquema conceptual general diseñado para este trabajo (ver

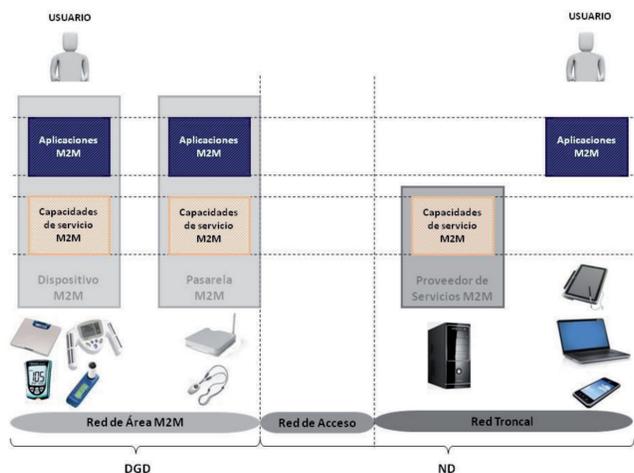


Fig. 1: Esquema conceptual V-H de la arquitectura M2M en el contexto de la e-Salud

Fig. 1). El flujo de información se indica con flechas (las discontinuas señalan opcionalidad) y en la explicación de cada paso se añade, entre paréntesis y cuando sea pertinente, el nombre de la capacidad de servicio M2M empleada. Además, en las figuras que se presentan en las siguientes secciones,

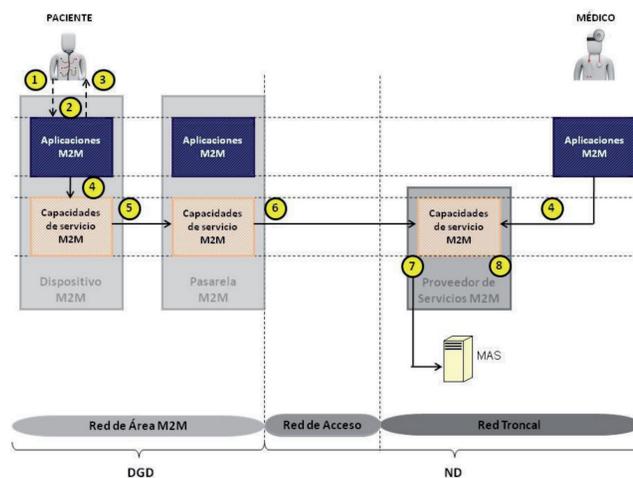


Fig. 2: Esquema conceptual de la inicialización y registro del dispositivo

RED DE ÁREA M2M	RED DE ACCESO	RED TRONCAL
1. El dispositivo M2M en el DGD puede necesitar físicamente la conexión a un equipo portátil o similar para llevar a cabo la transferencia inicial de información.		
2. El dispositivo M2M realiza un diagnóstico básico para asegurar que el dispositivo funciona correctamente. En aplicaciones críticas para la vida el dispositivo realiza una verificación integral bajo un entorno de ejecución seguro (DSEC).		
3. Un fallo en la inicialización lanza una señal de alarma al dispositivo y se bloquea el registro.		
4. Las aplicaciones M2M en el dominio DGD se registran de manera independiente en su dominio gracias a la entidad de capacidad de servicio correspondiente, de cara a iniciar la operación (DAE).		4. Las aplicaciones M2M en el dominio ND se registran de manera independiente en su dominio gracias a la entidad de capacidad de servicio correspondiente, de cara a iniciar la operación (NAE).
5. La capacidad de servicio correspondiente del dispositivo M2M envía una petición de registro al proveedor de servicio (DGC)	6. La pasarela M2M (si es aplicable) encamina la petición de registro hacia la red (GGC).	7. Las capacidades de servicio apropiadas en el ND realizan el registro, autenticación, y autorización de las aplicaciones M2M (NSEC), comprobando los datos con el Servidor M2M de Autenticación (M2M Authentication Server, MAS) que es donde se guarda la información de suscripción del usuario, y proporcionan conectividad a otras capacidades (NAE).
		8. Otras capacidades de servicio monitorizan el registro inicial y la desactivación del dispositivo o pasarela M2M, realizan la traducción de nombres, proporcionan el mapeo de nombres y direcciones monitorizando el estado del dispositivo (NRAR) y proporcionan selección de red a los dispositivos que soportan múltiples redes o servicios de comunicación (NCS).

Tabla II: Pasos explicativos de la inicialización y registro del dispositivo

se eliminan del diagrama los dibujos de los dispositivos para una mayor claridad y se identifica a los usuarios de los dominios DGD y ND (de forma global y siguiendo la explicación anterior) como ‘Paciente’ y ‘Médico’, respectivamente, para facilitar su asimilación (cuando sea necesario) a los agentes de los casos de uso a evaluar.

3. RESULTADOS

El ETSI define cuatro casos de uso: monitorización remota de pacientes (*Remote Patient Monitoring*, RPM), mensajería segura entre paciente y médico, medidas de señales corporales de muy baja tensión y tráfico de datos de teleasistencia entre el hogar y el Centro remoto de monitorización. Los tres primeros están suficientemente detallados como para trasladarlos a nuestro esquema conceptual V-H y redefinir los escenarios.

3.1. MONITORIZACIÓN REMOTA DE PACIENTES

Este primer caso de uso se centra en la comunicación desde el dispositivo remoto del paciente y las medidas recogidas

por los sensores hasta los sistemas que pueden ser accedidos por el médico, incluyendo los mensajes necesarios para su correcto funcionamiento. Dentro del caso de uso, se subdividen

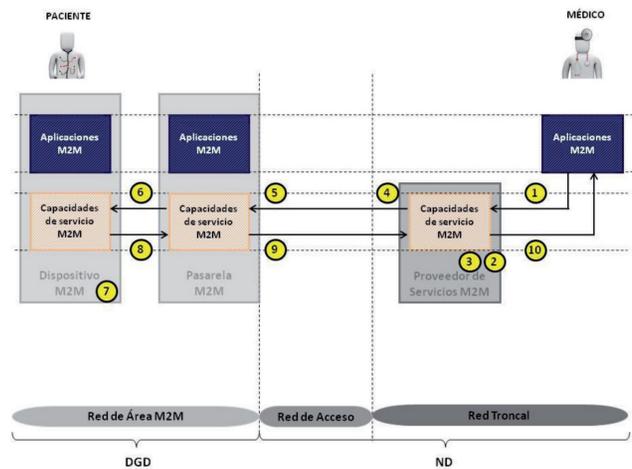


Fig. 3: Esquema conceptual del control remoto y configuración

RED DE ÁREA M2M	RED DE ACCESO	RED TRONCAL
		1. La entidad segura de autenticación, autorización y control de cuentas (Authentication, Authorization and Accounting, AAA) del ND, autentica y autoriza al usuario (NSEC).
		2. El mensaje se analiza para comprobar la identidad del receptor.
		3. La capacidad de servicio correspondiente confirma que el dispositivo está registrado, mira en el mapa de nombres su dirección de red y proporciona selección de red si el dispositivo soporta múltiples redes o servicios de comunicación (NCS). Después, las siguientes capacidades de servicio chequean el estado actual del dispositivo (si está disponible o no) y la última ruta conocida (NRAR), proporcionan registros de cargo según el uso de las capacidades (NAE) y ofrecen funciones de gestión de configuración (NREM).
6. La pasarela M2M en el DGD (si es aplicable) encamina el mensaje hacia el dispositivo M2M (GGC).	5. El mensaje pasa, a través de la pasarela M2M, si ésta fuera necesaria.	4. La capacidad de servicio apropiada envía los mensajes entre la aplicación y el dispositivo M2M (NGC). Se encarga de retransmisiones, informe de errores y monitoriza el estado de la entrega. Otra capacidad de servicio almacenará copias de los mensajes y otros detalles de la comunicación como el estado de la entrega y los informes de error (NRAR).
7. El dispositivo M2M recibe el mensaje		
8. La capacidad de servicio correspondiente del dispositivo M2M notificará al solicitante el estado de mensaje entregado y enviará la información requerida (p.ej. un médico que solicita una lectura de datos) (DGC).	9. La pasarela M2M (si es aplicable) encamina la respuesta hacia la red (GGC).	10. El mensaje se encamina hasta la aplicación de red (NGC)

Tabla III: Pasos explicativos del control remoto y configuración

tres escenarios: inicialización y registro del dispositivo (donde el dispositivo de monitorización remota queda listo para ser usado); control remoto y configuración (donde el dispositivo

de monitorización remota puede ser configurado o controlado a través de la red por medio de las aplicaciones M2M); y telemetría del paciente (el punto esencial de este caso de uso, en que el dispositivo de monitorización remota obtiene las medidas del paciente, datos, y/o eventos necesarios y los envía al médico).

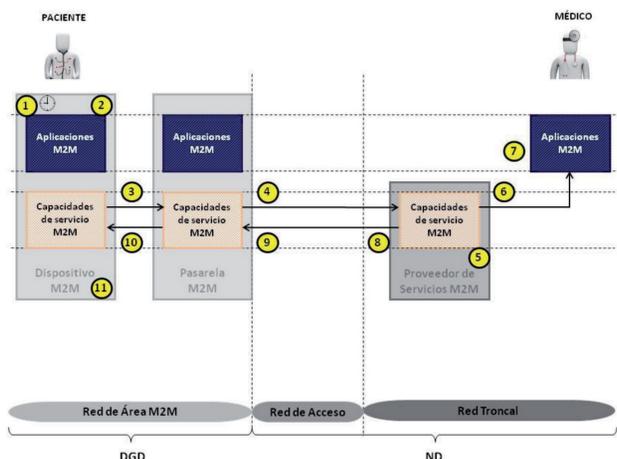


Fig. 4: Esquema conceptual de la telemetría del paciente

3.1.1. Inicialización y registro del dispositivo

Los pasos necesarios para inicializar y registrar el dispositivo M2M de monitorización remota y establecer la comunicación se muestran en la Fig.2 y se explican en detalle en la Tabla II. Se indica entre paréntesis la capacidad de servicio empleada en cada momento.

3.1.2. Control remoto y configuración

Este escenario describe la comunicación remota entre un usuario (p.ej. el médico) y un dispositivo y/o aplicación M2M. Los pasos a ejecutar son (ver Fig. 3 y Tabla III).

Además de los citados, si se tratara de un dispositivo M2M crítico para la vida del paciente, el manejo y entrega de mensajes deberá efectuarse en un tiempo mínimo.

RED DE ÁREA M2M	RED DE ACCESO	RED TRONCAL
1. De acuerdo a un horario predefinido o basado en algún evento, el dispositivo M2M en el DGD se "despierta" y se registra con la red (ver Fig. 2).		
2. Si la red es inalcanzable el mensaje se almacena y se intentará conectar con la red a intervalos predefinidos.		
3. Una vez conectado, el dispositivo M2M se prepara y envía el mensaje (DGC).	4. La pasarela M2M en el DGD (si fuera necesaria) encamina el mensaje hacia la red (GGC). De aquí en adelante, consideramos que hay una gestión inteligente de los datos transmitidos y asumimos que el mensaje llega al proveedor de servicio.	5. La capacidad de servicio adecuada da acceso al resto de capacidades necesarias y proporciona registros de cargo según el uso de las capacidades (NAE). La siguiente capacidad de servicio abstrae el nombre e información de conexión de la aplicación M2M y funciones de gestión. También monitoriza y proporciona funciones de configuración, rendimiento y gestión de errores (NREM).
		6. La capacidad de servicio correspondiente transportará el mensaje hasta la aplicación M2M en la red (NGC). Maneja retransmisiones, informes de error, oculta información innecesaria y monitoriza el estado de la entrega. Otra capacidad de servicio almacenará copias de los mensajes y otros detalles de la comunicación como el estado de la entrega y los informes de error (NRAR).
		7. La aplicación M2M en el ND recibe el mensaje.
10. La pasarela M2M en el DGD (si es aplicable) encamina el mensaje hacia el dispositivo M2M (GGC).	9. El mensaje pasa, a través de la pasarela M2M, si ésta fuera necesaria.	8. Se notifica el estado de mensaje entregado al dispositivo M2M en el DGD (NGC).
11. El dispositivo M2M recibe el mensaje		

Tabla IV: Pasos explicativos de la telemetría del paciente

3.1.3. Telemetría del paciente

Conceptualmente, este escenario describe la situación opuesta al anterior caso: comunicación desde un dispositivo M2M (o una aplicación instalada en él) hasta un usuario (o servicio M2M). Los pasos se muestran en la Fig. 4 y se detallan en la Tabla IV.

Además de los requisitos anteriores, un dispositivo M2M de monitorización remota crítico para la vida debe tener los siguientes: entrega fiable y garantizada de un mensaje; sincronización de tiempos precisa y segura; selección y uso de canales de comunicación adecuados para asegurar una transmisión confiable ante eventos críticos para la vida; entrega de mensajes de manera ordenada basada en el manejo priorizado de las distintas capacidades de servicio; y comunicaciones prioritarias con los servicios de emergencia.

3.2. MENSAJERÍA SEGURA ENTRE PACIENTE Y MÉDICO

Este caso de uso se refiere al intercambio de mensajes seguros entre paciente y médico (o staff médico) pero que involucran necesariamente al menos a un dispositivo M2M a o a una aplicación M2M, siempre bajo un entorno de envío y recepción seguro.

Estos mensajes seguros son soportados por el propio dispositivo M2M o aplicación M2M (a través de una capacidad de servicio M2M de mensajería segura) o por medio de una plataforma informática más genérica en el caso de que se vea involucrado el usuario (paciente o médico). Por ejemplo, un paciente puede tener un dispositivo de monitorización remota

de la salud que reporta datos fisiológicos y tener aparte una aplicación de mensajería segura que está basada en web y que se ejecuta desde un ordenador para mensajes iniciados por él de manera manual.

Aunque en TR 102732 se muestran más escenarios donde puede haber un intercambio de mensajes seguro (como el caso de un cambio de conexión producido al mover un dispositivo M2M a otra red o el seguimiento de su ubicación), nosotros nos centraremos en los tres definidos en más detalle: el regis-

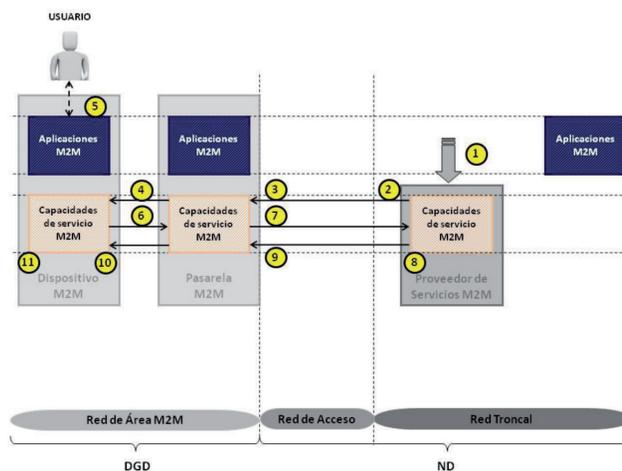


Fig. 5: Esquema conceptual del mantenimiento del dispositivo

RED DE ÁREA M2M	RED DE ACCESO	RED TRONCAL
		1. La capacidad de servicio responsable de la gestión de configuración (NREM) es alertada de que una actualización software está disponible para el dispositivo, a través de un proceso establecido entre el operador de red y el proveedor del dispositivo
4. La pasarela M2M en el DGD (si es aplicable) encamina el mensaje hacia el dispositivo M2M (GGC).	3. El mensaje pasa, a través de la pasarela M2M, si ésta fuera necesaria.	2. La capacidad de servicio correspondiente establece una conexión con el dispositivo y le envía un mensaje de que hay una actualización software disponible (NGC).
5. El dispositivo en el DGD aceptará, denegará o aplazará la actualización del software de acuerdo a lo establecido en su configuración (DREM). Puede ser necesaria la intervención del usuario.		
6. Una vez que el dispositivo acepta la actualización, se lo hace saber a la capacidad de servicio de red (DGC).	7. La pasarela M2M (si es aplicable) encamina la aceptación hacia la red (GGC).	8. La capacidad de servicio correspondiente descarga la actualización al dispositivo (NREM)
10. El dispositivo comprobará que la actualización software es válida y que está aprobada por las medidas de seguridad pertinentes (DREM).	9. La descarga pasa, a través de la pasarela M2M, si ésta fuera necesaria.	
11. Una vez que la descarga se ha completado, el dispositivo se reiniciará y comenzará la ejecución del nuevo software		

Tabla V: Pasos explicativos del mantenimiento del dispositivo

tro inicial de la capacidad de mensajería segura, la comunicación, y el mantenimiento del dispositivo. Como ya hemos comentado, todos los escenarios considerados deben soportar una comunicación iniciada por el usuario (paciente o médico) y una comunicación iniciada por el dispositivo (en base a un evento o a un horario programado).

3.2.1. Registro de la capacidad de mensajería segura

a) Registro del usuario: los pasos son muy similares al registro visto en RPM (ver Fig. 2), pero solo referidos a datos del usuario.

b) Registro del dispositivo: los pasos son virtualmente idénticos al registro en RPM (ver Fig. 2), porque ambos se refieren al registro del dispositivo (en este caso para enviar y recibir mensajes seguros).

3.2.2. Comunicación

a) Comunicación iniciada por el usuario: Un usuario (paciente o médico) inicia la comunicación con un dispositivo M2M o aplicación M2M (p.ej. un paciente que quiere actualizar su base de datos de salud con información relevante). Los pasos son casi idénticos al caso de control remoto y configuración de RPM (ver Fig. 3), aunque en este caso el contenido de los mensajes sea diferente a los de control o configuración.

b) Comunicación iniciada por el dispositivo: Un dispositivo M2M (o aplicación M2M) inicia la comunicación con otro dispositivo M2M (o aplicación) o con un usuario (p.ej. un dispositivo envía informes periódicos sobre ciertos datos fisiológicos a ciertas horas predeterminadas). Los pasos son casi idénticos a los del caso de telemetría de RPM (ver Fig. 4).

3.2.3. Mantenimiento del dispositivo

Este escenario describe los requisitos necesarios para la actualización del software o cualquier otro tipo de mantenimiento para el dispositivo M2M. Se presupone que el dispositivo tiene la capacidad de soportar una actualización al vuelo (*over the air*) y de almacenar una copia de seguridad del software, pudiendo volver a instalarla si hay un problema con la nueva actualización. Los pasos se muestran en la Fig. 5 y se explican en la Tabla V.

3.3. MEDIDAS CORPORALES DE MUY BAJA TENSIÓN

Este caso de uso podría considerarse un requisito previo dentro de un caso de monitorización remota de pacientes (RMP). Cuando se necesitan capturar las señales corporales de baja tensión con fines de monitorización remota de la salud, el proceso de adquisición podría llegar a perturbarse por las actividades de transmisión de radio (por ejemplo, en el caso de las aplicaciones de salud donde se están midiendo continuamente por un sensor inalámbrico las señales corporales para generar un electrocardiograma (ECG), la red corporal puede ser interferida por los transmisores GSM/GPRS pertenecientes a la pasarela M2M o co-ubicados en el propio dispositivo M2M).

Como se indica explícitamente en TR 102732, dependiendo del tipo de servicio M2M, una forma para hacer frente a las transmisiones de radio perturbadoras e inesperadas es muestrear simultáneamente un indicador de señal de la transmisión de radio, de cara a ajustar el proceso de muestreo de la señal, con el objetivo de reducir los efectos de la interferencia. Otra técnica, más eficiente en términos de energía, podría ser controlar el transmisor de radio mediante la suspensión de su transmisión durante el tiempo en que se estén produciendo las medidas, y luego reanudarla cuando la sesión de medidas concluya.

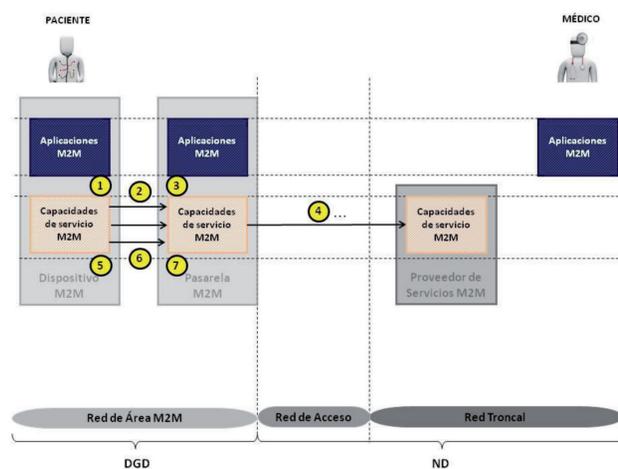


Fig. 6: Esquema conceptual de medidas corporales de muy baja tensión

RED DE ÁREA M2M	RED DE ACCESO	RED TRONCAL
1. Antes de comenzar la RPM, los transmisores en el dispositivo M2M (p.ej. GSM/GPRS) suspenden su actividad de transmisión radio (DREM).		
2. El dispositivo envía una señal de control a la pasarela M2M (DGC).		
3. Los transmisores en la pasarela M2M suspenden también su actividad de transmisión radio (GREM).		
4. Se realiza la RPM (ver sección 3.1.).		
5. Cuando la RPM concluye, los transmisores en el dispositivo M2M reanudan su actividad de transmisión radio (DREM).		
6. Se envía una señal de control a la pasarela M2M (DGC).		
7. Los transmisores en la pasarela M2M reanudan su actividad de transmisión radio (GREM).		

Tabla VI: Pasos explicativos de medidas corporales de muy baja tensión

Esto no solo evitaría interferencias, sino que disminuiría el consumo de energía, lo que puede ser esencial en aplicaciones críticas para la vida del paciente. Este camino está asociado al concepto de comunicación M2M 'green' [8], que pretende reducir el impacto medioambiental de los sistemas M2M.

La Fig. 6 y la Tabla VI muestran los pasos en una RPM para evitar interferencias en el DGD, teniendo en cuenta esta última consideración.

4. DISCUSIÓN Y CONCLUSIONES

El último caso de uso presentado en TR 102732 (tráfico de datos de teleasistencia entre el hogar y el Centro remoto de monitorización) cae fuera del ámbito de nuestro trabajo al estar presentado a muy alto nivel, sin detalles de la comunicación. Este caso de uso trata sobre cómo habilitar un enlace de comunicación IP para transmitir datos de teleasistencia (alarmas, muestreo de datos relativos a la actividad diaria, monitorización periódica de eventos) y transmisión bidireccional de voz entre el hogar (pasarela M2M) y el Centro de teleasistencia, por medio de un interface WAN, prestando especial atención a la definición de alarmas y mensajes de control, la mayoría de ellos en tiempo real. Todo ello supone habilitar gran cantidad de sensores y un incremento del tráfico generado. Sin embargo, al analizar este caso, vemos que el principal escollo a salvar es independiente de la carga de datos.

Hoy en día, el principal problema de los dispositivos médicos es la pluralidad de protocolos de comunicación establecidos por los proveedores. Por lo tanto, implementar futuros dispositivos M2M adaptados al Protocolo de Internet versión 6 (IPv6) y demás capas OSI (*Open Systems Interconnection*) puede ser una tarea muy difícil sin un estándar que los soporte. La estandarización tiene un impacto positivo de cara a incrementar la variedad de productos ofrecidos y el desarrollo de nuevas oportunidades de negocio. Además, como muchos estudios han indicado [9], los efectos de los estándares formales son significativamente mejor valorados por los actores implicados que otros tipos de estándares, como los informales o los propietarios de facto. Mediante la estandarización, no solo aumenta la capacidad para desarrollar soluciones M2M de una manera universal y colaborativa, sino que la creación de nuevos servicios M2M se simplifica enormemente.

En este contexto de asegurar la interoperabilidad entre dispositivos médicos que puedan usarse en un entorno M2M, la familia de normas ISO/IEEE 11073 [10], internacionalmente recomendada, puede ser un buen punto de partida ya que anticipa la estandarización entre dispositivos médicos, abstrayéndose de los canales de comunicación y permitiendo que interactúen independientemente entre ellos. En la misma línea que la propuesta planteada de esquemas conceptuales V-H y diagramas funcionales de comunicación estandarizada, la familia de normas ISO/IEEE 11073 incluye una serie de estándares que se agrupan en una arquitectura dividida en tres niveles:

1) Especialización de dispositivo (*Device Specialization*). Un conjunto de modelos descriptivos que aglutina el total de objetos y atributos relacionados con los componentes de los dispositivos, como la configuración global del sistema (*Medical Device System*, MDS), la métrica persistente (*PM-Store*) o las especificaciones de la métrica.

2) Protocolo optimizado de intercambio (*Optimized Exchange Protocol*). La parte principal del estándar que consiste en un marco de terminología médica y técnica (*Domain Information Model*, DIM) que se encapsulará dentro de una trama (*Protocol Data Unit*, PDU) sobre el que, después, un Modelo de Servicio define un conjunto de mensajes e instrucciones para obtener datos del agente basado en el DIM. Además, proporciona una conversión de datos de Sintaxis de Notación Abstracta (*Abstract Syntax Notation*, ASN.1) a una sintaxis de transferencia usando reglas de codificación (*Encoding Rules*, ER) optimizadas denominadas *Medical Device Encoding Rules* (MDER)

3) Capa de transporte (Transport Layer). La transmisión de datos es independiente de la tecnología de transporte. ISO/IEEE 11073 permite que todos los mensajes anteriormente planteados puedan transportarse a través de tecnologías como Bluetooth, USB, ZigBee, u otras futuras.

Como conclusión, en este artículo hemos creado un esquema conceptual de orientación vertical y horizontal (V-H) para describir de manera diáfana la arquitectura M2M en el ecosistema de la e-Salud. Con esta herramienta, hemos revisado los casos de uso explicados por el ETSI de cara a clarificar situaciones ambiguas, especialmente a la hora de nombrar las capacidades de servicio empleadas y situar las entidades en sus correspondientes dominios, para que su posterior implementación sea más sencilla. Nuestro análisis nos revela también dos puntos interesantes que pueden dar lugar a trabajos posteriores. Por un lado, la búsqueda por conseguir una mayor eficiencia energética en los dispositivos médicos implicados, nos sugiere una investigación más profunda en el concepto 'M2M green' orientado a la salud. Por otra parte, revisando el actual mercado de dispositivos médicos y su interoperabilidad, en los que algunos dispositivos inalámbricos ya se adaptan a las normas ISO/IEEE 11073, concluimos que estudiar estas directrices y vincularlas con el concepto de M2M, podría resultar un fructífero camino.

BIBLIOGRAFÍA

- [1] Miorandi D, Sicari S, De Pellegrini F, Chlamtac I. "Internet of things: Vision, applications and research challenges". *Ad Hoc Networks*. 2012. Vol.10-7. p.1497-1516. (DOI: <http://dx.doi.org/10.1016/j.adhoc.2012.02.016>).
- [2] "Internet de las cosas" DYNA. Septiembre 2014. Vol. 89-5 p.478
- [3] Boswarthick D, Elloumi O, Hersent, O. "M2M Communications: A Systems Approach". 1st ed. New York, Wiley, 2012. ISBN: 978-11-199-9475-6
- [4] Proyecto europeo epSOS. Available from <<http://www.epsos.eu/>>
- [5] eHealth Action Plan 2012-2020. Available from <http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=9156>
- [6] eHealth European Interoperability Framework. Available from <http://bookshop.europa.eu/is-bin/INTERSHOP.enfinity/WFS/EU-Bookshop-Site/en_GB/-/EUR/ViewPublication-Start?PublicationKey=KK0313200>
- [7] ITU-T. "General principles and general reference model for Next Generation Networks". Report n°: Y.2011, 2004. Available from <<http://www.itu.int>>
- [8] Lu R, Li X, Liang X, Shen X, Lin X. "GRS: The Green, Reliability, and Security of Emerging Machine to Machine Communication". *IEEE Communication Magazine*. 2011. Vol. 49-4. p.28-35. (DOI: <http://dx.doi.org/10.1109/MCOM.2011.5741143>).
- [9] Blind K, Gauch S, Hawkins R. "How stakeholders view the impacts of international ICT standards". *Telecommunications Policy*. 2010. Vol. 34. p.162-174. (DOI: <http://dx.doi.org/10.1016/j.telpol.2009.11.016>).
- [10] ISO/IEC/IEEE. "Health informatics Personal health device communication - Part 20601: Application profile - Optimized exchange protocol". Report n°: 11073-20601, 2011. Available from <<http://ieeexplore.ieee.org>>