Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes

PARTE 1: INTRODUCCIÓN

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO
ontsi observatorio nacional de las telecomunicaciones y de la SI

Este documento constituye una aproximación parcial al estudio de la interoperabilidad en nuestras ciudades; se enmarca dentro del *Servicio para el Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes* promovido por el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información, de Red.es, y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la información.

Para la realización de este estudio se ha contado con la colaboración de AT4 wireless S.A.U.

Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes

Año 2016

ÍNDICE

1. RESUMEN EJECUTIVO

La interoperabilidad es un elemento central en el desarrollo de las Ciudades Inteligentes. El Comité Técnico de Normalización AEN/CTN 178 "Ciudades inteligentes" movilizó un amplio consenso en la redacción de la norma: "Ciudades inteligentes. Infraestructuras. Sistemas Integrales de Gestión de la Ciudad Inteligente" (UNE 178 104)[10].

El presente estudio constituye una primera aproximación al conocimiento del concepto de interoperabilidad entre plataformas de gestión de servicios inteligentes. Se trata, por tanto, de un estudio parcial ya que está centrado en estándares que no tienen exactamente el mismo objeto, puesto que la Norma UNE 178 104 es más específica para la materia que el estándar oneM2M. Desde el Plan Nacional de Ciudades Inteligentes está previsto definir estudios que aborden con mayor profundidad los casos de aplicación que se consideren relevantes.

Este documento constituye la primera de las cuatro partes que componen el informe de dicho estudio y recoge una introducción a los principales conceptos que se abordan como son el concepto de interoperabilidad, las Plataformas de Gestión de Ciudades Inteligentes y los estándares de referencia.

Respecto al concepto de Interoperabilidad, no existe una definición única que satisfaga a todos, pero se puede concluir que la interoperabilidad puede ser considerada como la capacidad de dos o más sistemas o componentes para intercambiar datos y utilizar la información intercambiada [1].

En la creación de estándares y programas de prueba y validación, la interoperabilidad debe ser tenida en cuenta desde el principio para la definición de requisitos, considerándola un objetivo fundamental.

El concepto de Plataformas de Gestión de Ciudad Inteligente se recoge en la norma UNE 178 104 [10]. Una Plataforma de Gestión de Ciudad Inteligente debe facilitar los servicios a los ciudadanos, a la vez que procurar la máxima eficiencia de la Administración y un fácil despliegue técnico en el entorno de las Ciudades Inteligentes.

Es fundamental que los servicios de la Ciudad Inteligente estén soportados por una Plataforma que asegure el correcto funcionamiento de éstos, además de su eficiencia, rendimiento, seguridad y escalabilidad.

Los objetivos principales de una Plataforma Integral de Ciudad Inteligente son:

- Recoger la información de la Ciudad, ciudadanos y empresas, cumpliendo los requisitos de privacidad que fueran pertinentes.
- Distribuir la información, para que pueda ser procesada por los responsables de los diferentes servicios.
- Analizar la información según los criterios definidos
- Tomar decisiones devolviendo la información refinada a los sistemas encargados de ejecutar las distintas acciones.

- Exponer datos y capacidades a desarrolladores para facilitar la creación de un ecosistema de aplicaciones sobre la plataforma, que cree un valor adicional para el ciudadano.

Entre los objetivos del presente estudio se establece que las Plataformas de referencia para el mismo son las propuestas para la Gestión de Ciudades Inteligentes por:

- Thinking City de Telefónica [3]
- IOC de IBM [8]
- SmartBrain de Abertis (ahora Cellnex Telecom) [5]
- Sofia2 de Indra [4]
- Wonderware de Schenider-electric [7]
- Carriots de Wairbut [6]

En este documento se incluye una breve descripción de cada una de ellas.

Igualmente, en esta introducción se incluye un resumen de los principales estándares de referencia que se han tenido en cuenta para la elaboración de este Estudio. Son los siguientes:

- UNE 178 104 (AENOR). “Ciudades Inteligentes. Infraestructuras. Sistemas integrales de gestión de la Ciudad Inteligente” [10]
- UNE 178 301 (AENOR). “Ciudades Inteligentes. Datos abiertos” [11]
- TS-0001 (oneM2M). “Functional Architecture”. V1.6.1 [12]
- TS-0002 (oneM2M). “Requirements” V1.0.1 [13]
- TR-0001 (oneM2M). “oneM2M Use Cases Collection” V0.0.5 [14]

2. OBJETIVOS DEL DOCUMENTO

El objetivo final es buscar la portabilidad y reutilización de las aplicaciones y la compartición de dispositivos sobre las diferentes Plataformas de Gestión de Ciudades Inteligentes. Este estudio constituye una primera aproximación al conocimiento del concepto de interoperabilidad entre plataformas de gestión de servicios inteligentes. Desde el Plan Nacional de Ciudades Inteligentes está previsto definir estudios que aborden con mayor profundidad los casos de aplicación que se consideren relevantes.

Además se pretende conocer el posible impacto de la estandarización que se está llevando a cabo tanto a nivel nacional, en el CTN 178 de AENOR, como internacional, en el oneM2M, y sus posibles consecuencias en el desarrollo de soluciones Smart Cities en España, y tomar, a partir de las conclusiones de este Estudio, las medidas que se consideren oportunas.

El Estudio se ha dividido en tres fases:

- **E1: FASE 1**

  1. **Identificación de puntos de referencia (o confluencia de estándares)** entre los que se puede establecer comparativa entre el modelo de capas propuesto en el documento UNE 178 104 de AENOR y la arquitectura oneM2M.

  2. Definición de una **metodología de análisis y cumplimiento de requisitos** para diferentes plataformas comerciales y casos de uso frente a los estándares de referencia.

  3. **Analizar Casos de Uso** reales implantados en diferentes ciudades nacionales conforme establece oneM2M. Los Casos de Uso seleccionados son:

     - Automatización manejo de iluminación en exteriores (calles, etc.)
     - Servicio de compartición de bicicletas
     - Smart Parking
     - Gestión Semafórica
     - Riego inteligente

- **E2: FASE 2**

  Elaboración de **cuestionarios** de cumplimiento de requisitos frente a los estándares de referencia que permitan identificar diferentes grados de compatibilidad con los mismos.

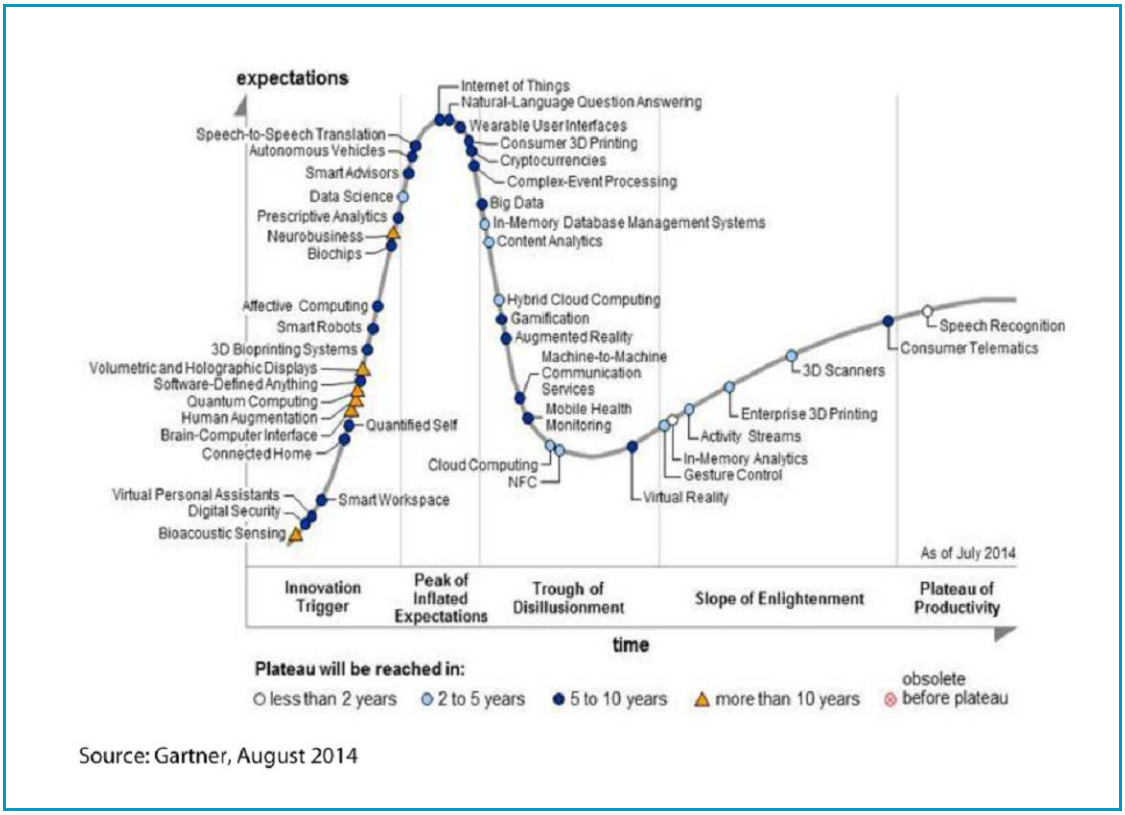
- **E3: FASE 3**

  Propuesta de **soluciones interinas** que pudieran ser utilizadas para asegurar la interoperabilidad de las plataformas seleccionadas, en los casos de uso anteriores, minimizando en lo posible los costes de desarrollo, pero siempre admitiendo, a medio plazo, una evolución hacia los estándares propuestos en oneM2M.

Para completar el Estudio, se han generado cuatro documentos, uno introductorio a los conceptos de interoperabilidad, Plataformas de Gestión y estándares de referencia, que está constituido por el presente documento, y otros tres correspondientes a cada una de las Fases definidas en el Estudio.

3. INTEROPERABILIDAD

No hay duda de que dentro de unos años, habrá un gran aumento del número de dispositivos conectados. La firma de análisis Gartner sitúa a la IoT en la parte superior de su ciclo para tecnologías emergentes y anticipa 5 años la llegada a la plena madurez del mercado respecto a previsiones anteriores [2].



Source: Gartner, August 2014

Existen dos factores claves para que se cumplan estas expectativas: por un lado la reducción de precios de los dispositivos y servicios y por otro el acceso a los mismos de los usuarios finales, que van a requerir aspectos como la seguridad, la escalabilidad y la interoperabilidad sean reales.

Reconocida por todos los agentes la necesidad de la estandarización y normalización en relación a estas tecnologías emergentes, es prioritario crear la infraestructura y metodología necesaria para la verificación y validación frente a estos estándares, actualmente en desarrollo a nivel nacional e internacional, de los productos y servicios relacionados con ellas.

Hay organismos nacionales e internacionales, públicos y privados inmersos en las tareas de definición de estándares poniendo “orden” en las tecnologías relacionadas con las Ciudades inteligentes.

Uno de los motivos subyacentes para el desarrollo de estándares de comunicación es facilitar la interoperabilidad entre los productos en un multi-proveedor, multi-red y entorno multi-servicio.

Son estas las demandas del mercado que han asegurado que la interoperabilidad ha mantenido, de hecho aumentado, su protagonismo en la normalización.

La interoperabilidad garantiza que los usuarios tienen una mayor oferta de productos y que los fabricantes pueden beneficiarse de las economías de escala que un mercado más amplio les ofrece.

No existe una definición única de la interoperabilidad que satisfaga a todos, pero se puede concluir que la interoperabilidad puede ser considerada como la capacidad de dos o más sistemas o componentes para intercambiar datos y utilizar la información intercambiada [1].

En la creación de estándares y programas de prueba y validación, la interoperabilidad debe ser tenida en cuenta desde el principio para la definición de requisitos, considerándola un objetivo fundamental.

La interoperabilidad de los productos que cumplen con las normas sólo puede garantizarse si además:

- *Las Interfaces y arquitecturas están completamente definidas en las normas*
- *Las especificaciones han sido bien definidas*
- *Los protocolos especificados son robustos, flexibles y eficientes*
- *El comportamiento especificado, los formatos de datos y las codificaciones son claras y sin ambigüedades.*
- *El contexto en el que se utilizan las especificaciones se entiende completamente*
- *Las especificaciones se revisan y mantienen adecuadamente*

Una vez que un conjunto de requisitos se ha identificado y definido, es importante validar que, de hecho, ofrecen una solución estandarizada interoperable. Algunas organizaciones plantean, para validar las normas en sí, pruebas prácticas como eventos de interoperabilidad, o Plugfests.

Las pruebas son una parte importante a la hora de proporcionar una garantía de interoperabilidad. Hay tres niveles de actividades de prueba relacionadas que deben ser consideradas y que se abordan en los otros documentos que componen este Estudio [15]:

1. **Pruebas de conformidad:** garantizan que un producto implementa correctamente el estándar y es capaz intercambiar información con otra aplicación utilizando un protocolo conocido o conjunto de protocolos.

2. **Pruebas de interoperabilidad:** se realizan por medio de dispositivos de diferentes fabricantes y conexión entre ellos, ya sea manual o automáticamente, de acuerdo con escenarios basados en un protocolo estándar.

3. **Certificación:** garantiza que un producto puede legalmente afirmar haber implementado una norma correctamente.

4. PLATAFORMAS DE GESTIÓN DE SERVICIOS

4.1. CONCEPTO DE PLATAFORMA DE GESTIÓN DE CIUDAD INTELIGENTE

Como se recoge en el UNE 178 104 [10][9], una Plataforma de Gestión de Ciudad Inteligente debe facilitar los servicios a los ciudadanos, a la vez que procurar la máxima eficiencia y una fácil integración en el entorno de las Ciudades Inteligentes.

Es fundamental que los servicios de la Ciudad Inteligente estén soportados por un Plataforma que asegure el correcto funcionamiento de éstos, además de su eficiencia, rendimiento, seguridad y escalabilidad.

Los objetivos principales de una Plataforma Integral de Ciudad Inteligente según la norma UNE 178 104:

- *Recoger la información de la Ciudad, ciudadanos y empresas, cumpliendo los requisitos de privacidad que fueran pertinentes.*
- *Distribuir la información, para que pueda ser procesada por los responsables de los diferentes servicios.*
- *Analizar la información según los criterios definidos*
- *Tomar decisiones devolviendo la información refinada a los sistemas encargados de ejecutar las distintas acciones.*
- *Exponer datos y capacidades a desarrolladores para facilitar la creación de un ecosistema de aplicaciones sobre la plataforma, que cree un valor adicional para el ciudadano.*

Las plataformas avanzadas simplifican el desarrollo de aplicaciones, reduciendo los tiempos de desarrollo y los costes de mantenimiento. Permiten la adopción de estándares de mercado y hacen los desarrollos más reusables y extensibles. Además estas plataformas permiten el análisis integrado del rendimiento y la seguridad de las aplicaciones lo que permite a los responsables municipales realizar una gestión más eficiente de todos sus recursos.

La UNE 178 104 de AENOR se centra en los requisitos que se deben cumplir para permitir:

1) El conocimiento en tiempo real de la realidad de la ciudad.
2) La coordinación y puesta a disposición de la información disponible por parte de los gestores de los servicios de mantenimiento de la ciudad.
3) La gestión dinámica de las actividades de acuerdo a datos reales, recursos disponibles y niveles objetivos de calidad de los servicios.
4) La gestión de la calidad de los servicios a través del seguimiento de indicadores, con una visión global y transversal.
5) La eficiencia y sostenibilidad: debe permitir ajustar los recursos aplicados a las necesidades precisas de cada área, asegurando el cumplimiento de los niveles de calidad objetivos.

6) El establecimiento de los canales de interacción con el Gobierno de la Ciudad y con los Ciudadanos a través de subsistemas específicos que establezcan flujos bidireccionales de información

La Plataforma debe proporcionar los elementos necesarios para que se garanticen los requisitos anteriores:

- Independencia entre aplicaciones y dispositivos. Las aplicaciones desarrolladas no deben depender del fabricante concreto de los dispositivos de sensorización y control.
- Interoperatividad entre servicios verticales. Tanto la información como los propios dispositivos empleados por un servicio vertical concreto deben poderse usar por otros verticales y servir de base para aplicaciones avanzadas en la ciudad. Este es el sentido fundamental de una plataforma horizontal.
- Las plataformas deben proveer una serie de servicios comunes de forma estandarizada. De este modo se evita la duplicidad funcional y es esperable una mayor calidad técnica en los componentes desarrollados por empresas especializadas.

De forma adicional, es deseable:

- Separación entre la lógica de las aplicaciones y sus implementaciones concretas.
- Existencia de implementaciones abiertas de referencia.

La plataforma debe soportar Monitorización y Operación centralizada, segura y multiusuario sobre los diferentes recursos, elementos o sistemas de una ciudad, permitiendo:

1) Acceso a los datos de plataformas de sensores, bases de datos y a información de otras aplicaciones.
2) Actuaciones sobre actuadores (sensores) a través de soluciones estandarizadas.
3) Registro de las diferentes actividades que se desarrollan en el sistema.
4) Acceso a las aplicaciones de los sistemas tipo SCADA para la gestión de la energía y usos de toda la ciudad (fuentes, iluminación, gestión de edificios, etc.).
5) Mantenimiento de equipos e infraestructuras.
6) Soporte de protocolos estándar de monitorización como SNMP o JMX.
7) Integración con otros sistemas o casos de uso como:
    - Control semafórico
    - Transporte público
    - Estaciones meteorológicas y medioambientales (emisiones, ruido, vibraciones, movimientos de tierra por satélite, etc.)
    - Producción de energía
    - Fuentes
    - Gestión de agua (riego, alcantarillado, pozos, etc.)
    - Recogida de basuras

- Videovigilancia
- Aparcamiento público y en superficie
- Sistemas de acceso (acceso identificado a edificios, pilonas, peajes, pago por uso,...)
- Sistemas de gestión de flotas (municipales, bicicletas, car- share, taxi, etc.)
- Puntos de recarga del VE (vehículo eléctrico)
- Sistemas de información ciudadana (sistemas de quejas, notificación de incidencias en la vía pública, emergencias urbanas, redes sociales o turismo) y CRMs
- Redes sociales
- ERP corporativo
- GIS
- Sistemas de sensorización

De cara al fomento de la interoperabilidad, las plataformas deben:

- Proveer las interfaces necesarias para que eventos de un sistema puedan desencadenar acciones en otros
- Usar APIs y protocolos normalizados (MQTT, REST,etc.)
- Soportar la capacidad de extenderse para incluir nuevos protocolos de comunicación (CoAP, STOMP, etc.)

A continuación, a modo ilustrativo, se muestra una descripción general de algunas de las Plataformas consideradas en este Estudio, basada en información pública de las mismas.

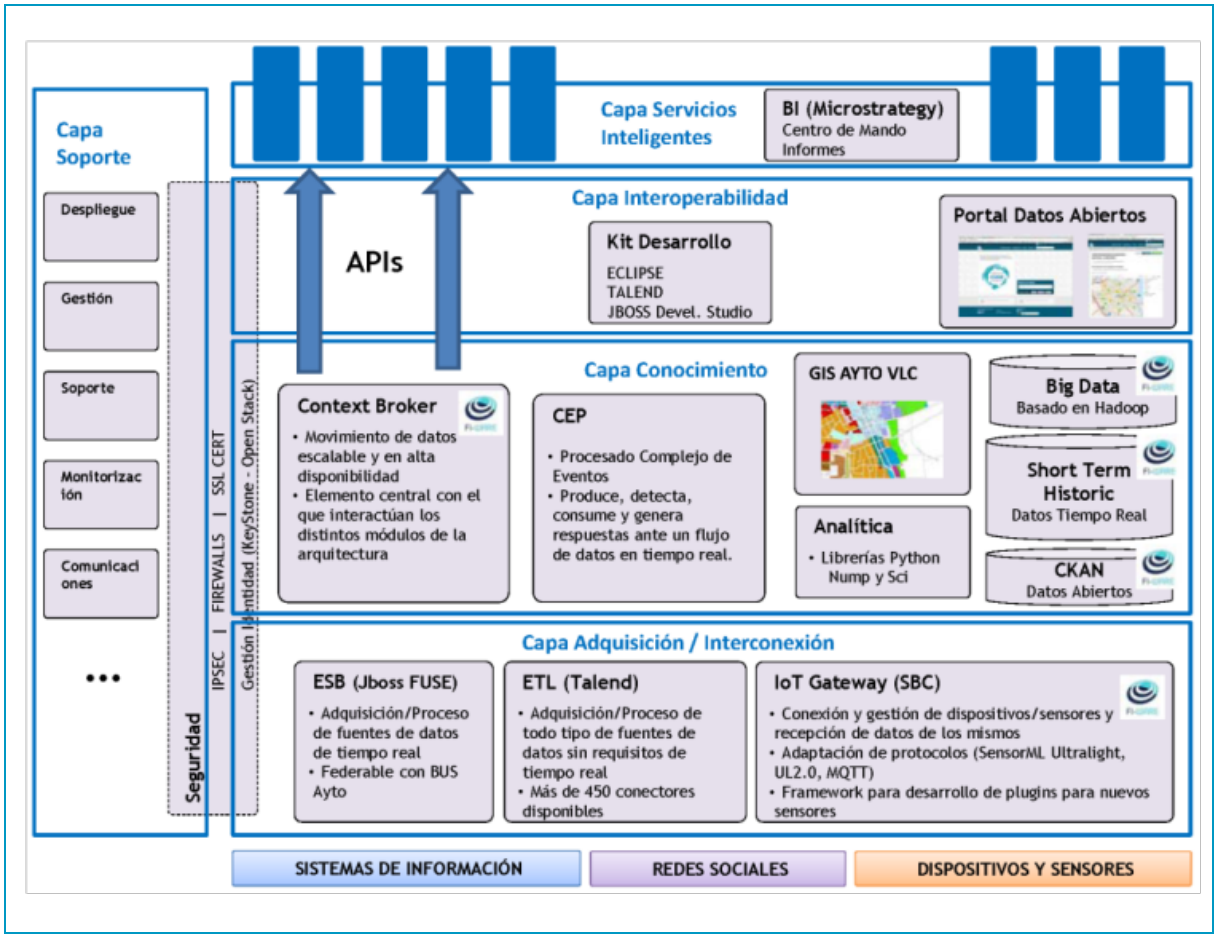
4.2. Plataforma Thinking City (Telefónica)

Thinking City [3] es la solución para Smart Cities de Telefónica, basada en su plataforma IoT (Internet-of-Things). Dicha plataforma es compatible con FIWARE, es decir se basa en los correspondientes “enablers” genéricos disponibles a través de la iniciativa FIWARE (www.fiware.org) y está alineada con su filosofía de plataforma horizontal, abierta y basada en estándares.

Incorpora:

- APIs que proveen de interfaces abiertos NGSI mediante los que se da acceso a la capa de servicios a los datos y capacidades de la capa de conocimiento.
- Kit de Desarrollo: Eclipse, TALEND, JBOSS Developer Studio.
- Portal Datos Abiertos: portal de acceso a los datos abiertos de la ciudad.
- Cuadros de mando basados en Microstrategy para la variedad de servicios que puede desplegar la ciudad sobre la plataforma: transporte (paneles informativos, aparcamientos, servicio municipal de bicicletas, etc.), gestión de infraestructuras (riego, iluminación, etc.), seguridad y emergencias, etc.

A continuación se muestra un esquema de la arquitectura de Plataforma de Gestión Thinking city de Telefónica.



4.3. PLATAFORMA IOC (IBM)

El Centro de Gestión Inteligente (IOC) de IBM® [8] proporciona un Cuadro de Mandos (dashboard) para ayudar a los gestores y responsables de la ciudad a tener una mayor percepción de la ciudad en diferentes aspectos de la gestión.

Ofrece visualización de datos integrada, colaboración casi en tiempo real y analítica exhaustiva para ayudar a las ciudades a mejorar la eficiencia continua de sus operaciones, planificar su crecimiento y gestionar los trabajos de respuesta. IBM Intelligent Operations Center proporciona mapas integrados, paneles de instrumentos en línea, informes personalizables, múltiples algoritmos de analítica, procedimientos operativos estándar interactivos y otras herramientas para mejorar las operaciones de la ciudad y la respuesta ante incidentes o emergencias.

IBM Intelligent Operations Center permite:

- Supervisar operaciones a lo ancho de la ciudad y contestar a eventos e incidencias recibidas a través de agentes.
- Involucrar a los ciudadanos y empresas en la notificación y resolución de los incidentes
- Agrupar y analizar una retroalimentación de los ciudadanos a través de las redes sociales

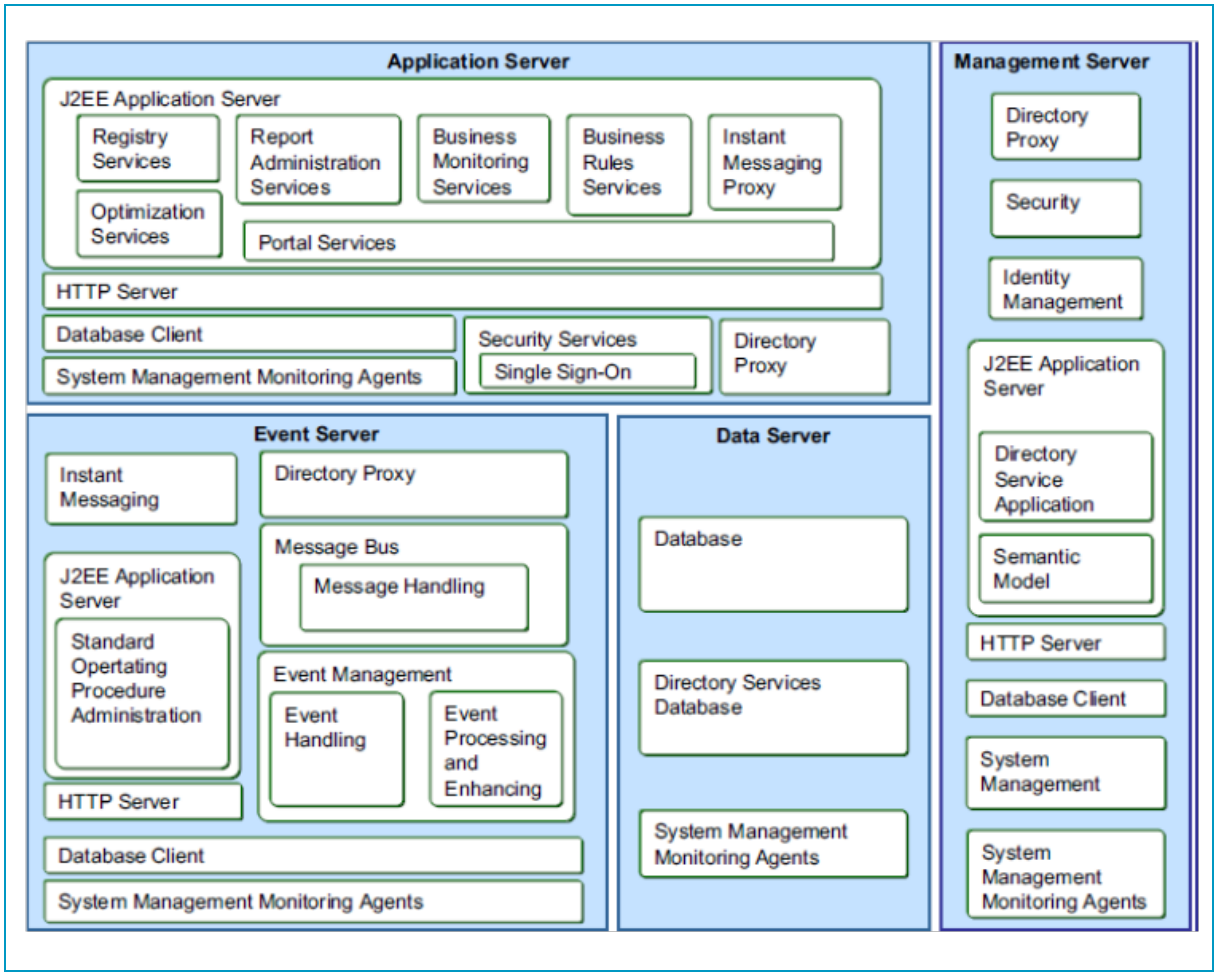
- Gestionar un amplio rango de operaciones de la ciudad
- Desplegar rápidamente con mínimos recursos IT

IBM Intelligent Operations Center usa la potencia de los datos generados en el mundo real para:

- Recopilar y gestionar los datos correctos
- Integrar y analizar los datos
- Facilitar acceso a la información fácil y puntual
- Ajustar los sistemas para alcanzar los resultados basados en percepciones adquiridas

El Intelligent Operation Center (IOC, Centro de Gestión de la Ciudad Inteligente) proporciona medidas, monitorización y herramientas de modelado que integran sistemas subyacentes en una solución para mejorar la eficiencia operacional, planificación y coordinación.

A continuación se muestra un esquema de arquitectura de la Plataforma IOC [9] .



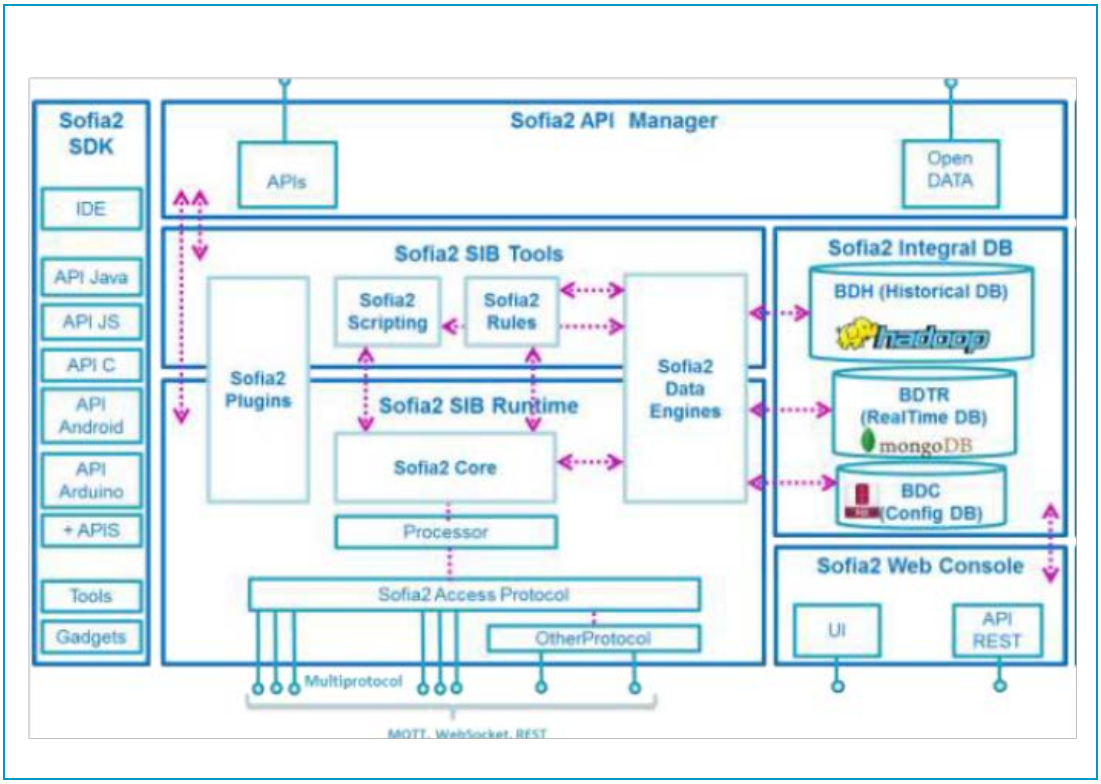
4.4. PLATAFORMA SOFIA2 (INDRA)

Sofia2 [4] es un middleware que permite la interoperabilidad de múltiples sistemas y dispositivos, ofreciendo una plataforma semántica que permite poner información del mundo real a disposición de aplicaciones inteligentes (Internet of Things).

SOFIA (SMART OBJECTS FOR INTELLIGENT APPLICATIONS) surge como un proyecto I+D Artemis de tres años (finalizado en marzo de 2012) en el que han participado 19 partners de cuatro países de la UE incluyendo Nokia, Philips, Fiat y Acciona.

Indra Sofia2 Smart Platform, la Plataforma Smart Cities de Indra, es una Plataforma global que aplica no sólo al ámbito Smart Cities, aunque este sea uno de sus ámbitos de aplicación.

A continuación se muestra un esquema modular de la arquitectura de Sofia2.



Sofia2 es multilenguaje y multiprotocolo, permitiendo así la interconexión de dispositivos heterogéneos. Proporciona mecanismos de publicación y suscripción, facilitando la orquestación de sensores y actuadores para monitorizar y actuar sobre el entorno.

Sofia2 es:

- Open-source
- Multiplataforma: disponible para Windows, Android, Linux, iOS,...
- Multilenguaje: con portings a Java, Javascript, C++, Arduino
- Agnóstica de las comunicaciones: con implementaciones TCP, MQTT, HTTP (REST y WebServices), Ajax Push,...

- Multidispositivo, a través de su SDK, API's y mecanismos de extensión que permite su integración con cualquier tipo de dispositivo.

Se basa en los siguientes estándares:

- JSON (JavaScript Object Notation): Formato de texto para intercambio de información entre sistemas, muy ligero y adecuado para dispositivos (Arduino, móviles,etc.), empleado por muchas plataformas Open DATA basadas en JSON
- Servicios REST y RESTful. APIS Web como evolución de Servicios SOA
- Hadoop

4.5. Plataforma SmartBrain (Cellnex Telecom)

SmartBrain [5] es un servicio de Cellnex Telecom que garantiza el acceso a las infraestructuras urbanas mediante la homogeneización de los datos recopilados en distintas fuentes. Consta de una infraestructura informática de diseño modular con estándares abiertos y de una serie de aplicaciones en la nube que garantizan y posibilitan el intercambio de datos, con lo que puede usarse de forma simultánea por parte de distintos usuarios con diferentes perfiles (ciudadanos, administración, grupos de interés social, distribuidores, desarrolladores, etc.). Es una herramienta para potenciar la participación y los servicios do-it-yourself para los ciudadanos, así como para mejorar la interacción con la administración y la transparencia.

Su diseño modular, los estándares abiertos y el uso de interfaces API y del kit SDK facilitan su integración con otras aplicaciones de desarrollo nuevas o ya existentes, con lo que se reduce el tiempo de puesta en el mercado de los nuevos Servicios de la Ciudad. A continuación se muestra un esquema modular de SmartBrain.

Las principales características que ofrece son:

- Solución abierta, no relacionada con un vendedor concreto.
- Resiliencia del servicio.
- Intercambio de datos e información desde todas las áreas de la Administración.
- Adaptación a las necesidades y sistemas de la ciudad.
- Reducción del tiempo de creación de los servicios públicos.
- Mejora de la transparencia y la participación.
- Facilitación de la transformación de la Administración.
- Creación de nuevos modelos de relaciones y de negocios.
- Intercambio de datos e información entre la ciudad y los desarrolladores.

Con el objetivo de conseguir la máxima facilidad y flexibilidad la plataforma ofrece los servicios de acceso siguiendo los siguientes estándares/esquemas de integración:

- API Web Services utilizando una interfaz en formato XML SOAP basada en el estándar Basic Profile de la organización Web Services Interoperability (WS-I).
- API basada en RESTful Web Services.

- SDK que encapsula el uso de las APIs para su desarrollo en .NET (Silverlight) y simplifica la implementación de aplicaciones ofreciendo códigos de ejemplo y notas técnicas de soporte.

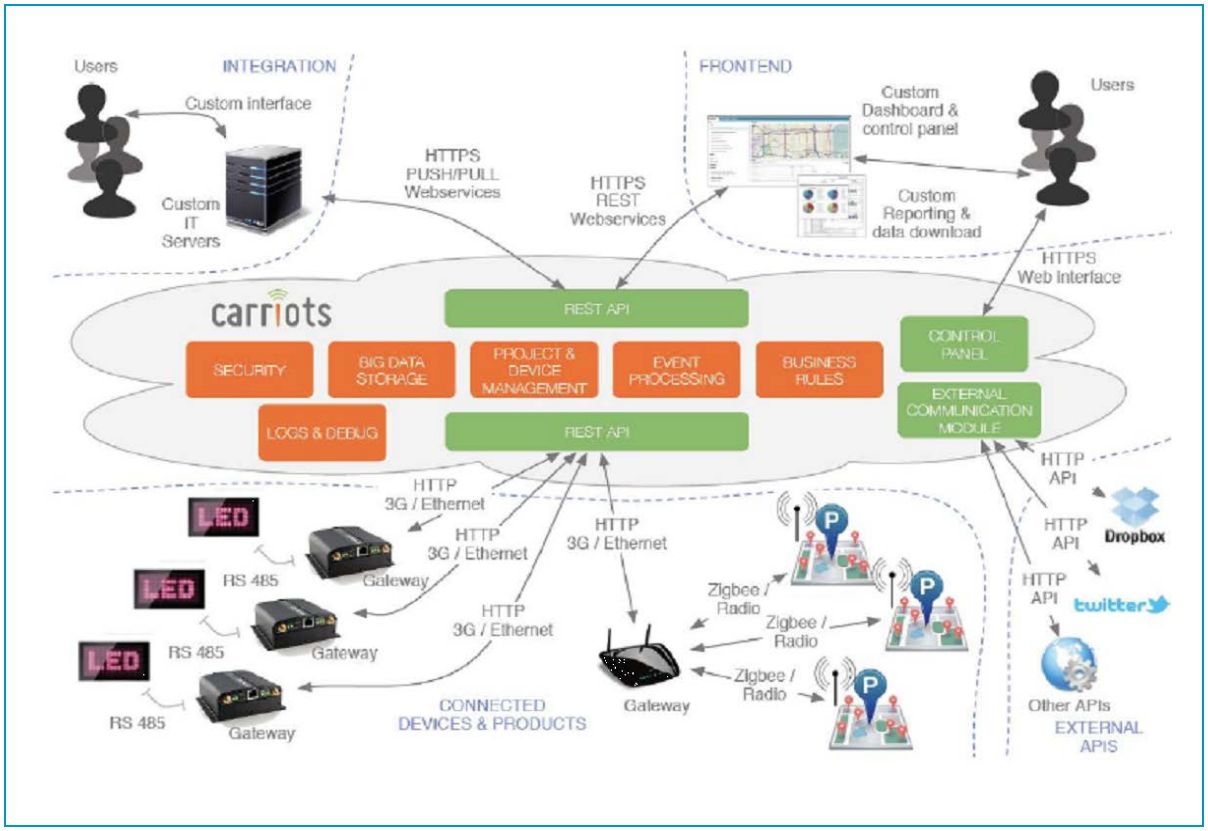
4.6. Plataforma Carriots (Wairbut)

Carriots [6] es una Plataforma como Servicio (PaaS en sus siglas en inglés) diseñada para proyectos del Internet de las Cosas (IoT) y de Máquina a Máquina (M2M).

Sus características principales son:

- Recolección de datos. Almacenamiento de datos de sus sensores o la información de estado del dispositivo a través de HTTP API REST y XML o JSON.
- Almacenamiento. Base de datos NoSQL con acceso a través de APIs. Permite almacenamiento y publicación de la información.
- Gestión de dispositivos. Permite mantener de forma remota, control e interactuar con dispositivos, independientemente de su ubicación.
- Interacción con otros sistemas: a través de los estándares REST API y web services.
- Reglas de negocio y procesamiento de eventos. La lógica de un proyecto IoT se mantiene y ejecuta en la plataforma. El motor ejecuta scripts Groovy, de forma aislada, basado en reglas asociadas a eventos del tipo if-then-else.

El siguiente diagrama muestra la vista general del sistema Carriots con sus principales componentes.



4.7. Plataforma Wonderware (Schneider Electric)

Wonderware System Platform [7] ofrece una plataforma común y escalable para cubrir las necesidades de información y automatización industrial relacionadas con Soluciones de Software SCADA, HMI de Supervisión, MES y EMI.

Dentro de Wonderware existe un historiador de procesos de alto desempeño con almacenamiento de historia de producción, compresión eficiente de datos y autoconfiguración de almacenamiento histórico que elimina la duplicación de esfuerzos, además de un servidor de gestión de información industrial vía web que simplifica la organización y presentación de información de operaciones.

Beneficios:

- La estandarización en el entorno de desarrollo y ejecución de operaciones ahorra tiempo y dinero
- Integración de todos los datos de operaciones, independientemente de su fuente
- Flexibilidad y capacidad para modificar cualquier aspecto del sistema para satisfacer nuevas necesidades o aprovechar nuevas oportunidades
- Escalabilidad para gestionar sistemas con tamaños desde 250 hasta más de 1 millón de conexiones I/O, independientemente de su ubicación geográfica

Capacidades

- El uso de un modelo de planta común reduce la complejidad
- Mantenimiento y despliegue remoto del software
- Extensible y fácil de mantener usando estructuras orientadas a objetos y a base de plantillas
- Poderoso modelo de seguridad a base de roles
- Características de comunicación y redes "optimizadas para SCADA"
- Recolección de datos históricos y capacidades de graficas avanzadas
- Capacidades para generación de reportes de base web

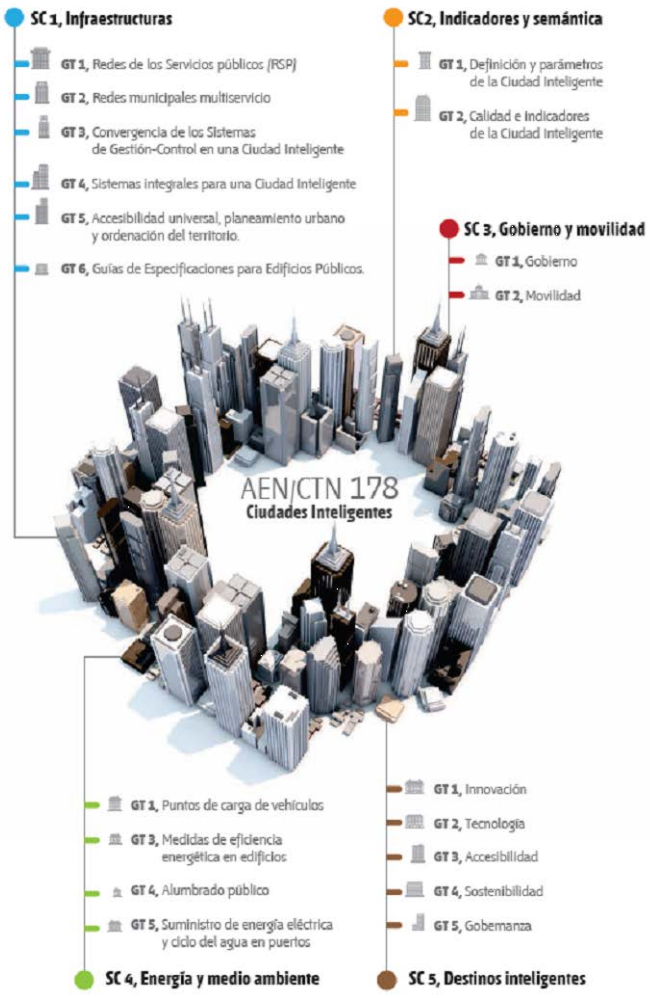
5. ESTÁNDARES DE REFERENCIA

5.1. GENERAL

Los Organismos de Normalización están en plena ebullición de producción de estándares.

En España, para ayudar a abordar las cuestiones relacionadas con el desarrollo de las ciudades inteligentes, SETSI, junto con el Comité Técnico de Normalización AEN/CTN 178 "Ciudades inteligentes", está desarrollando una estrategia de normalización para Ciudades Inteligentes o Smart Cities en España. La estrategia identifica el papel de las normas en la aceleración de la consecución de las Ciudades Inteligentes, asegurando a los ciudadanos una adecuada gestión de los riesgos.

El Comité Técnico de Normalización AEN/CTN 178 "Ciudades inteligentes" de AENOR tiene en su programa de trabajo la elaboración de un conjunto de normas que cubra las necesidades de las Ciudades Inteligentes, para ello ha definido una serie de subcomités que a su vez se dividen en Grupos de Trabajo, que se muestran en la figura siguiente [18]:



La Agenda Digital publicada por el Ministerio de Industria, Turismo y Energía marca la hoja de ruta en materia de Tecnologías de la Información y las Comunicaciones (TIC) y de Administración Electrónica para el cumplimiento de los objetivos de la Agenda Digital para Europa en 2015 y en 2020, e incorpora objetivos específicos para el desarrollo de la economía y la sociedad digital en España. Recoge en su Objetivo 5 "Impulsar el sistema de I+D+i en Tecnologías de la Información y las Comunicaciones", e incrementar la eficacia de la inversión pública en I+D+i. Según la Agencia Digital Europea, por cada millón de euros invertidos en TIC's en Europa se generan hasta 33 puestos de trabajo y su implementación para Europa permitirá crear 1,2 millones de puestos de trabajo en el corto plazo y hasta 3,8 en el largo plazo.

En España, muchas empresas TIC han invertido en el desarrollo de productos y servicios innovadores, basados en el uso de Plataformas de gestión, y para ello han contado con ayudas públicas tanto nacionales como internacionales.

Para lograr la eficacia de la inversión realizada es necesario fomentar la internacionalización de dichos resultados por lo que como pieza clave e imprescindible se considera el cumplimiento con los estándares internacionales y la capacidad de interoperabilidad de dichas Plataformas.

A nivel internacional, recientemente, diferentes organismos de estandarización, y más en concreto, la Asociación oneM2M (que integra los principales organismos de estandarización: ARIB, ATIS, CCSA, ETSI, TIA, TTA, TTC), está desarrollando las normas europeas para las comunicaciones M2M (Máquina-Máquina) e IoT, ambos elementos clave para su aplicación en el nuevo concepto de las Smart Cities por el que tan fuertemente se está apostando a nivel internacional.

Los primeros estándares han sido publicados a principios de 2015, pero diferentes grupos de trabajo siguen desarrollando las especificaciones e informes técnicos necesarios para garantizar la adecuación e interoperabilidad de los sistemas.

Por otro lado, asociaciones internacionales de fabricantes definen sus propios protocolos de comunicación y modelos de certificación entre dispositivos M2M para garantizar la interoperabilidad total como último objetivo. Algunos ejemplos pueden ser Allseen Alliance u Open Interconnect Consortium (OIC).

Los estándares de referencia de especial interés para la realización de este Estudio son:

- UNE 178 104 (AENOR). "Ciudades Inteligentes. Infraestructuras. Sistemas integrales de gestión de la Ciudad Inteligente" [10]
- UNE 178 301 (AENOR). "Ciudades Inteligentes. Datos abiertos" [11]
- TS-0001 (oneM2M). "Functional Architecture". V1.6.1 [12]
- TS-0002 (oneM2M). "Requirements" V1.0.1 [13]
- TR-0001 (oneM2M). "oneM2M Use Cases Collection" V0.0.5 [14]

A continuación se muestra un pequeño resumen del contenido de cada uno de ellos.

5.2.UNE 178 104

La norma UNE 178 104 de AENOR "Ciudades Inteligentes. Infraestructuras. Sistemas integrales de gestión de la Ciudad Inteligente" [10] atiende a la necesidad de normalización de los sistemas integrales de gestión de una Ciudad Inteligente planteada por el CNT178 de AENOR.

Este proyecto de norma se centra en los requisitos de intercambio de información y operación para que los sistemas cumplan con los objetivos exigibles para ellos, y en particular en lo referente a su seguridad, interoperabilidad, eficiencia, rendimiento y escalabilidad.

La norma establece la definición, los requisitos, las interfaces y las medidas para impulsar el despliegue de ciudades inteligentes en España y la reutilización de las aplicaciones ya desarrolladas.

La norma se divide en 4 bloques, que se sintetizan en los apartados siguientes:

- Vista funcional
- Vista tecnológica
- Métricas
- Anexos informativos

5.2.1. BLOQUE 1: VISTA FUNCIONAL

En este bloque de la norma se analizan cuáles son los objetivos de una Ciudad Inteligente y a continuación que características funcionales debe considerar una Plataforma Integral para facilitar dichos objetivos, ya que va a constituir la pieza fundamental de gestión de las Ciudades. Posteriormente se realiza una descripción funcional de lo que debe incluir una Plataforma:

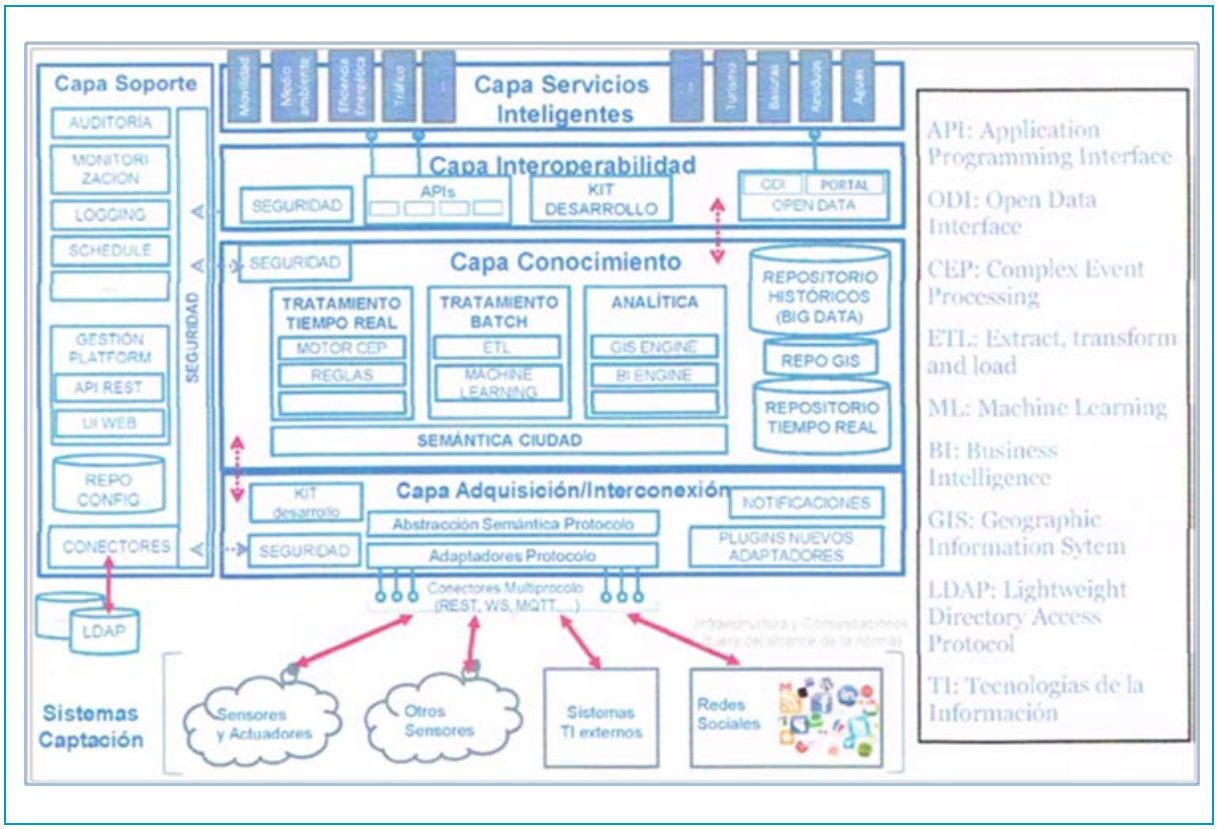
- Repositorio completo y actualizado de la información de la ciudad
- Gestión de las infraestructuras
- Comunicación entre sistemas
- Seguridad
- Herramientas de mantenimiento
- Soporte a la decisión
- Aplicaciones comunes (costes, informes, optimización y planificación, etc…)
- Difusión de la información en tiempo real
- Resistencia a fallos

5.2.2. BLOQUE 2: VISTA TECNOLÓGICA

En el bloque 2 de la norma se citan los requisitos técnicos que deben cumplir las plataformas:

1. **Horizontalidad**: capacidad de soporte de diferentes ámbitos de aplicación, de manera que sea posible la implementación simultánea de múltiples servicios en la misma infraestructura.
2. **Interoperabilidad**: capacidad de soporte de diferentes tecnologías, dispositivos y mecanismos de captura de información, y estándares de comunicación, así como otros sistemas de información internos/corporativos y/o externos.
3. **Rendimiento**: habilidad del sistema para manejar en tiempo real un elevado número de dispositivos, servicios y procesos de manera eficiente.
4. **Escalabilidad**: capacidad de poder incrementar capacidad de proceso y almacenamiento sin tener que modificar la arquitectura.
5. **Robustez y Resiliencia**: capacidad para seguir funcionando ante problemas
6. **Seguridad**: garantías del sistema en cuanto a seguridad, privacidad y confianza se refiere.
7. **Modularidad**: la plataforma debe tener un enfoque modular que permita desplegar por partes de forma sencilla
8. **Continuidad operativa o disponibilidad**: capacidad del sistema para estar operativo en cualquier momento
9. **Capacidad de Recuperación**: capacidad para gestionar de forma eficiente los fallos que puedan afectar a la disponibilidad.
10. **Flexibilidad**: habilidad de la plataforma para funcionar en diferentes escenarios y áreas
11. **Extensibilidad**: capacidad de la plataforma para poder ampliarse para dar soporte a nuevas necesidades
12. **Semántica**: el uso de conceptos semánticos en la Plataforma permite la interoperabilidad entre plataformas y por tanto entre ciudades
13. **Capacidades Big Data**: para integrar un gran cantidad de datos generados desde múltiples fuentes y con diferentes estructuras
14. **Basada en estándares abiertos**: lo que simplifica la integración con otras plataformas y el desarrollo de aplicaciones sobre la Plataforma que puedan ser reusables y portables entre diferentes plataformas.
15. **Evolucionable**: facilitando su capacidad de extensión en el futuro mediante estándares ampliamente adoptados.
16. **Integral**: la plataforma debe trabajar como un todo, no como piezas desacopladas que no están preparadas para trabajar en conjunto
17. **Operable y gestionable**: la plataforma debe poder gestionarse, operar, mantenerse e instalarse de forma sencilla.

Así mismo, se propone una aproximación a la estructura de capas para las Plataformas de Ciudades Inteligentes, que es la siguiente:



En la figura parecen los siguientes módulos de más alto nivel:

- **Sistemas de captación:** la forman las redes de sensores y actuadores, sistemas externos, redes sociales, etc.
- **Capa de adquisición/interconexión:** ofrece los mecanismos para la captación de datos desde los sistemas de captación y abstrae la información con un enfoque semántico estándar.
- **Capa de conocimiento**: recibe datos de las capas de adquisición e interoperabilidad y ofrece el procesado de datos, la incorporación de valor y la transformación de servicio.
- **Capa de interoperabilidad:** ofrece interfaces y conectores para que los sistemas externos puedan acceder a la plataforma y permite construir servicios a partir de los datos. Para ello debe ofrecer la API nativa de acceso a los datos de la capa de conocimiento.
- **Capa de servicios inteligentes:** está constituida por los servicios municipales conectados a través de la capa de interoperabilidad. Estos servicios pueden formar parte de la Plataforma o ser externos
- **Capa de soporte:** ofrece servicios comunes como auditoria, monitorización, seguridad, etc.

De cara a los objetivos de este Estudio son de **especial relevancias las capas de adquisición y de interoperabilidad**, ya que son las encargadas de ofrecer intercambio de información con otras aplicaciones y dispositivos.

Referente a la capa de adquisición se plantean dos modelos para dicha capa: el modelo ETSI y el modelo oneM2M.

Según se recoge en la norma UNE 178 104 para cumplir con el modelo ETSI deben incluirse:

- Interfaces abiertos y normalizados
- Una capa de adquisición única
- Independencia de la tecnología de acceso y de los sensores. Mediante protocolos abiertos, traducción de protocolos y debe ser posible añadir nuevos conectoras según avance la estandarización.

Respecto al modelo oneM2M, se recomienda que la capa de adquisición contemple un módulo de compatibilidad con las especificaciones oneM2M y valora diferentes niveles de interoperabilidad:

- a nivel de aplicación
- a nivel de datos (semántica)
- entre plataformas de servicios
- a nivel de dispositivos
- entre dispositivos

Además, en la norma, se recomienda identificar el nivel de interoperabilidad para diferentes casos de uso sobre plataformas existentes en el mercado.

Respecto a la capa de interoperabilidad, debe ofrecer interfaces y funcionalidades para garantizar la portabilidad de aplicaciones:

- Publicar APIs que puedan consumirse en la capa de servicios (API manager)
- Interconectar con aplicaciones y plataformas
- Acceder a servicios externos
- Publicar datos abiertos
- Permitir construir servicios a través de kit de desarrollo con SDK y APIs
- Integrar seguridad en todos los intercambios

Se recomienda que las APIs sean API REST. Deben soportar distintos modos de acceso como Push (subscripción y notificación) y Pull (petición respuesta) e igualmente soportar consultas geo-referenciadas. Para el modelo de datos se recomienda utilizar el propuesto por oneM2M.

Como último punto de este bloque de la norma, se analiza la interoperabilidad entre plataformas. Para ello las plataformas deben ser independientes en tres dominios:

- Independencia en el dominio de las aplicaciones
- Independencia en el dominio de la red
- Independencia en el sistema de adquisición

Finalmente se identifican problemas de interoperabilidad actuales en aspectos como:

- Plataformas que se conciben como sistemas de adquisición y tratamiento de datos (IoT, SCADA), no incluyen algoritmos inteligentes de predicción o aprendizaje.
- Tienden a mantener dependencia entre aplicaciones, dispositivos y red de transporte.
- Se puede decir que hay plataformas abiertas (no propietarias), pero el concepto de horizontalidad está aún lejano.
- Alguna de las plataformas plantean la integración de verticales existentes como fuentes de datos externas y no una verdadera interoperabilidad. No se integran directamente los sensores, sino las salidas del sistema que los gestionan.
- A veces se interpreta como interoperabilidad a nivel de aplicaciones el dotar de cierta capacidad de personalización de la interfaz al usuario, permitiendo el funcionamiento de la aplicación.
- A nivel semántico, se requiere una semántica común de intercambio de información. Hay una importante barrera en la normalización de éstos parámetros. Para lograr una verdadera interoperabilidad transversal y entre los verticales, se requiere gran trabajo de normalización, vocabularios y metadatos comunes que permitan implantar un verdadero Open Data
- En cuanto a la interrelación de la Plataforma con los subsistemas externos y aplicaciones verticales y con módulos adicionales, avanzados o de futuro, de la propia plataforma, muchas veces la integración de los sistemas verticales existentes y propietarios es una de las barreras de entrada al mercado de las plataformas horizontales en la Smart City.
- En cuanto a la propiedad se pueden encontrar:
    - Sistemas propietarios de un proveedor con interfaces también propietarias
    - Sistemas con núcleo propietario de un proveedor con interfaces exteriores abiertas
    - Sistemas con núcleo propietario de un proveedor con interfaces interiores (entre módulos del propio sistema de gestión integral) y exteriores abiertas
    - Sistemas con núcleo en código abierto 100% libre

5.2.3. BLOQUE 3: MÉTRICAS

En este apartado de la norma simplemente se citan las capacidades que hay que valorar:

1. Grado de adecuación al modelo de capas y funcionalidades

2. Modularidad de la Plataforma.
3. Integración con otras Plataformas.
4. Basarse en estándares abiertos.
5. Protocolos IoT soportados.
6. Capacidad de extensión de la Plataforma.
7. Soporte Enfoque Big Data
8. Soporte Enfoque Opendata
9. Servicio en On premise/cloud.
10. Inclusión capacidades GIS.
11. Inclusión de herramientas de uso y configuración.
12. Niveles de disponibilidad y nivel de servicio
13. Garantía, soporte y hoja de ruta

5.2.4. ANEXOS

Se añaden un anexo informativo de referencias de parámetros de interoperabilidad semántica.

5.3. UNE 178 301

La norma UNE 178 301 “Ciudades Inteligentes. Datos abiertos” [11] ha sido la primera norma del comité técnico AEN/CTN178 de Ciudades Inteligentes publicada por AENOR. Su objetivo es evaluar la publicación de datos abiertos por parte de las Administraciones públicas en el ámbito de las Ciudades Inteligentes.

Establece un conjunto de métricas que sirven de base para el cálculo de indicadores. Se han establecido 4 niveles:

- Nivel 0: Resultados inexistentes. No existe iniciativa de apertura o los resultados no son suficientemente relevantes.
- Nivel 1: Resultados incipientes. Existe una iniciativa informal de apertura de datos y estos son relevantes.
- Nivel 2: Resultados existentes. Existe una iniciativa formal de apertura de datos y estos son relevantes.
- Nivel 3: Resultados avanzados. Existe una iniciativa formal de apertura de datos que implementa las mejores prácticas.

Se han establecido 5 dominios sobre los que aplicar datos abiertos:

- Dominio estratégico

- Dominio legal
- Dominio organizativo
- Dominio técnico
- Dominio económico y social

Cada uno de estos dominios se ha clasificado en dimensiones y se han definido los niveles para cada uno de ellos. En particular, el dominio técnico establece los criterios para evaluar los protocolos y mecanismos que garanticen la disponibilidad de los datos y el grado de interoperabilidad.

En el apartado 5 del documento, Indicador de datos abiertos, se establece el cálculo de la puntuación final basada en los niveles alcanzados en cada una de las métricas.

Como anexo informativo incluye el conjunto de datos considerado como prioritario y los vocabularios de referencia.

5.4.TS-0001 ARQUITECTURA FUNCIONAL

La Especificación Técnica TS-0001 V1.6.1 "Functional Architecture" [12] ha sido publicada por oneM2M en Enero de 2015 y especifica la arquitectura funcional de las Plataformas de Servicios oneM2M, incluyendo la descripción de las entidades funcionales y los puntos de referencia asociados.

5.4.1. DEFINICIONES

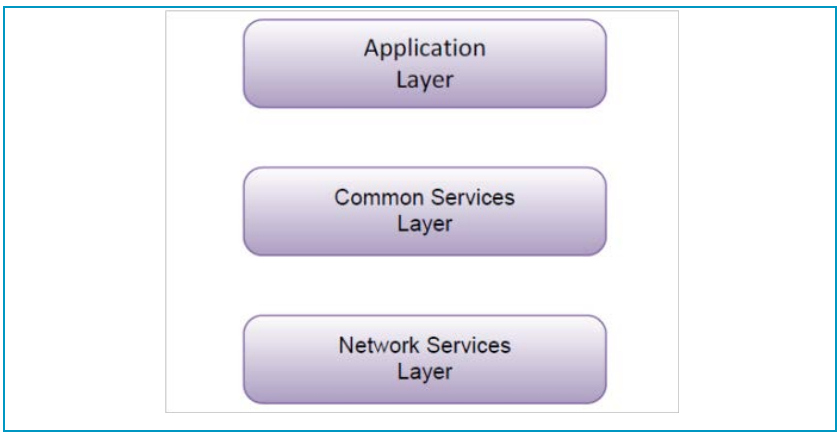
Es importante conocer las definiciones que se incluyen en la especificación para su comprensión total.

- **Activación de dispositivos (Device Triggering)**: Es un medio por el cual un nodo en el dominio de la infraestructura envía información a un nodo en el dominio de campo para realizar una tarea específica (por ejemplo para activar un dispositivo, para establecer la comunicación desde el dominio del campo hacia el dominio de infraestructura, o cuando la dirección IP para el dispositivo no está disponible o no es accesible).
- **Atributo:** Almacena información perteneciente a un recurso. Un atributo consta de un nombre y un valor.
- **Capa de aplicación:** Comprende las aplicaciones oneM2M, la lógica operacional y negocios relacionados.
- **Capa de servicios comunes:** consta de funciones de servicio oneM2M que permiten aplicaciones oneM2M (ej. Gestión, descubrimiento y la aplicación de políticas.
- **Capa de servicios de red:** Proporciona funciones de transporte y conectividad.
- **CSE Point of Access (CSE-PoA):** El CSE-PoA será utilizado por el Sistema M2M para comunicarse con un CSE en un nodo M2M. Una vez que se logra la comunicación con un CSE, una AE registrada con ese CSE puede ser contactada siempre y cuando la AE pueda ser identificada de forma única. La información incluida en el CSE-PoA así como la actualización del CSE-PoA depende de las

características de la red subyacente y las capacidades de transporte del nodo M2M.

5.4.2. MODELO DE CAPAS

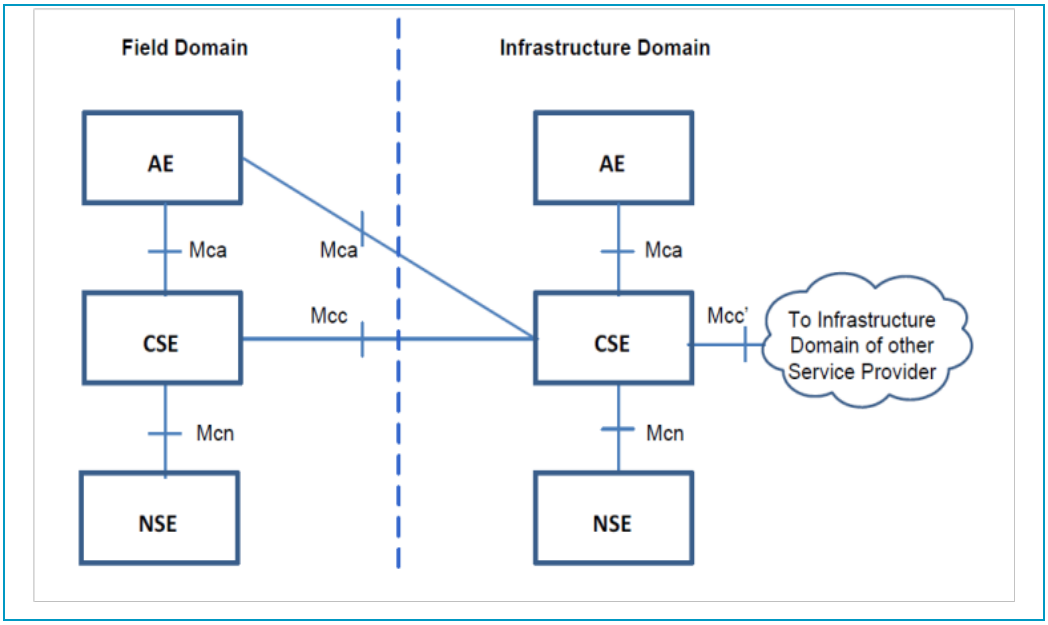
El modelo de capas para soportar Servicios M2M end-to-end se muestra en la siguiente figura:



El modelo de referencia de la arquitectura engloba la arquitectura funcional (entidades funcionales) y los puntos de referencia, que se describen a continuación.

5.4.3. ENTIDADES FUNCIONALES

La arquitectura funcional propuesta se muestra en la siguiente figura:



Los tipos de entidades funcionales son 3:

AE (Application Entity): Es una entidad en la capa de aplicación que implementa la lógica de servicio de una aplicación M2M y tiene un único identificador AE-ID. Algunos

ejemplos pueden ser: aplicación de gestión de flotas, aplicación de monitorización remota de la glucosa, aplicación de medida de consumo, etc.

CSE (Common Services Entity): Es una entidad que representa una instancia de un conjunto de funciones de servicios comunes en el entorno M2M y están identificadas unívocamente como CSE-ID. Estos servicios comunes son ofrecidos al resto de entidades. Algunos ejemplos son: gestión de datos, gestión de dispositivos a nivel de servicio, gestión de subscripciones o servicios de localización.

NSE (Network Service Entity): Ofrece servicios desde la red subyacente a los CSE. Algunos ejemplos son: gestión de dispositivos a nivel de red o triggering de dispositivos.

5.4.4. PUNTOS DE REFERENCIA

Un **punto de referencia** consiste en uno o más interfaces de cualquier tipo. Los principales puntos de referencia son los siguientes:

- **Mca Reference Point**: La comunicación fluye entre una CSE y una AE. Permite a la AE usar servicios de la CSE y a la CSE comunicar con la AE, pueden estar o no dentro de una misma entidad física.
- **Mcc Reference Point**: La comunicación fluye entre dos CSE. Permite usar servicios de otra CSE.
- **Mcn Reference Point**: La comunicación fluye entre una CSE y una NSE. Permite a a usar servicios de soporte (distintos del transporte y la conectividad) proporcionados por el NSE
- **Mcc´ Reference Point**: La comunicación fluye entre dos CSE en los nodos de la infraestructura proporcionadas por diferentes proveedores.

5.4.5. NODOS

En el apartado 6 del estándar de referencia [12] se analizan los aspectos de la arquitectura oneM2M.

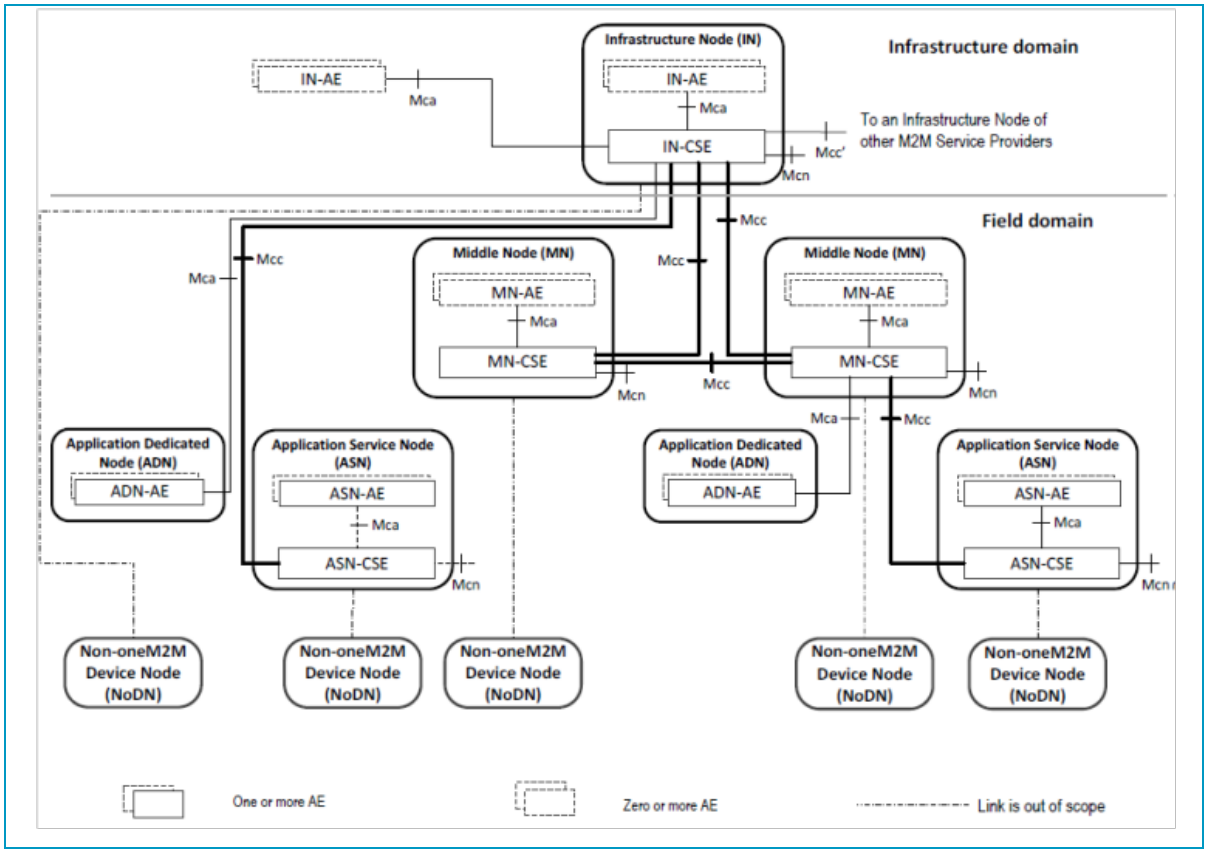
En primer lugar se detallan las configuraciones que puede soportar la arquitectura oneM2M para interconectar los distintos tipos de entidades y se introduce el concepto de **Nodo**. Los nodos son entidades lógicas individualmente identificables en un sistema oneM2M y pueden ser de varios tipos:

- **Application Service Node (ASN)**: Contiene un CSE y al menos una AE. Un ejemplo puede ser un dispositivo M2M.
- **Application Dedicated node (ADN)**: Contiene al menos un AE y no contiene ningún CSE. Como ejemplo un ADN puede residir en un dispositivo M2M.
- **Middle Node (MN)**: Contiene un CSE y cero o más AEs. Como ejemplo se puede considerar un Gateway M2M.

- **Infrastructure Node (IN)**: Contiene un CSE y cero o más AEs. Hay un IN en el dominio de la infraestructura por cada proveedor de servicio. Un ejemplo puede ser una infraestructura de servicios M2M (o Plataforma).

- **Non-oneM2M Node (NoDN)**: Es un nodo que no contiene entidades oneM2M. Representan dispositivos adjuntos a un sistema oneM2M para interoperar con el sistema.

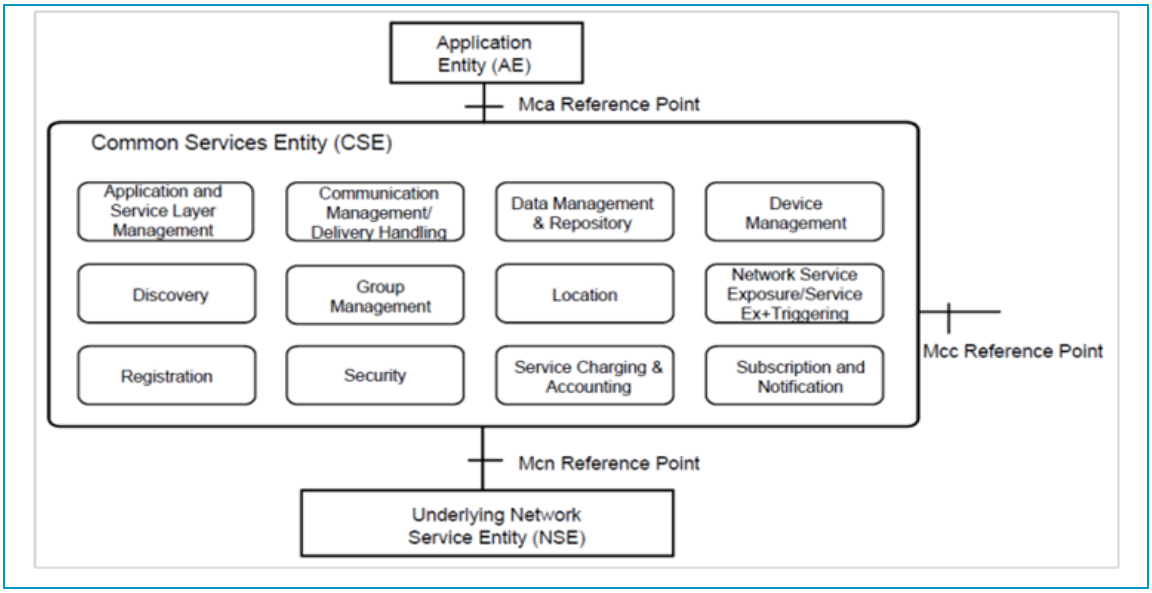
A continuación se muestra una figura donde se representan los nodos y entidades de una arquitectura oneM2M.



Hay un IN (nodo de infraestructura) por cada proveedor de servicio. EL CSE del IN contiene lo que se denominan funciones CSF (Common Service Function), no aplicables a otro tipo de nodos.

5.4.6. FUNCIONES DE SERVICIOS COMUNES

Los servicios proporcionados por la Capa de servicios comunes se reflejan en la siguiente gráfica y se denominan CSFs (Common Services Functions). La comunicación entre los diferentes CSF no se tratan en la especificación TS-0001, pero si sus interfaces con AE a través de Mca y con NSE a través de Mcn como con otros CSE.



A continuación se muestra un resumen de cada una de las funciones de una CSE. Son las siguientes

Application and Service Layer Management (ASM): Incluye las capacidades de configurar y gestionar el software y sus componentes para AEs y CSEs.

Communication Management and Delivery Handling (CMDH): Se encarga de gestionar la comunicación con otros CSEs, AEs o NSEs. Transporta los datos a un destino específico según los parámetros con los que los reciba. Decide la red de comunicación basándose en los servicios de subscripción y selecciona la ruta de comunicación y monitoriza la disponibilidad de las redes de comunicación.

Data Managemement & Repository (DMR): Se encarga del almacenamiento de datos y las funciones de mediación. Tiene capacidades para recoger y agregar datos y convertirlos a un formato específico y almacenarlos para su procesamiento analítico y semántico.

Device Management (DMG): Se encarga de la gestión de las capacidades de los dispositivos de nodos MN, ADN y ASN.

Discovery (DIS): Busca información sobre aplicaciones y servicios contenida en los atributos y los recursos.

Group Management (GMG): Se encarga de gestionar las peticiones de grupos relacionados.

Location (LOC): Permite a los AEs obtener información geográfica de los nodos (ASN o MN).

Network Service Exposure, Service Execution and Triggering (NSSE): Gestiona las comunicaciones con la red subyacente para acceder a los servicios de red a través de la interfaz Mcn como por ejemplo device triggering, pequeñas transmisiones de datos, notificaciones de localización reglas, etc…

Registration (REG): Procesa peticiones desde un AE u otro CSE para registrarse y poder acceder a los servicios.

Security (SEC): Se encarga de gestionar los datos sensibles, administrar la seguridad, establecer asociaciones de seguridad, controla los accesos y gestiona las identidades.

Service Charging and Accounting (SCA): Proporciona las funciones de carga de la capa de servicios.

Subscription and Notification (SUB): Proporciona notificaciones relativas a una suscripción que sigue los cambios en un recurso.

En los apartados siguientes de la especificación se analizan los aspectos de seguridad, y comunicaciones dentro de un mismo sistema M2M o entre sistemas de diferentes proveedores y la suscripción a servicios, se define el modelo de identificación de objetos y entidades y se describen los flujos sobre los puntos de referencia, la gestión de recursos y flujos de información.

Finalmente hay varios Anexos informativos de interés como son el mapeo de requisitos sobre las CSFs, la comunicación entre el sistema y la red subyacente o la interoperación/integración con soluciones y protocolos no oneM2M.

5.5.TS-0002 Requisitos

Este documento [13] contiene, a nivel informativo, un modelo de roles funcionales y a nivel normativo los requisitos técnicos para oneM2M.

Los requisitos se agrupan de la siguiente manera:

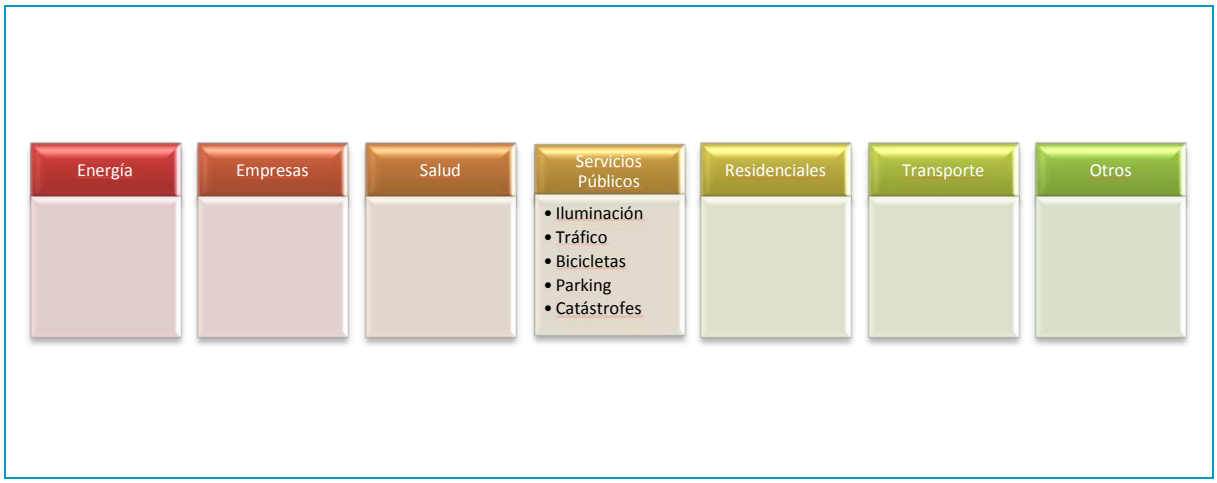
- OSR: Overall system requirements
- MGR: Management requirements
- ABR: Abstraction requirement
- SER: Security requirement
- CHG: Charging requirment
- OPR: Operational requirement
- CMR: Communication management requirement

5.6.TR-0001 Casos de uso

En la versión 2013-Sep-23 del TR-0001 [14], que es la última versión publicada hasta el momento. Se recogen los casos de uso M2M de diferentes segmentos industriales. Se agrupan en:

- Energía
- Empresas
- Salud
- Servicios Públicos

- Residenciales
- Transporte
- Otros casos de uso



Dentro del grupo de servicios públicos, que es el considerado para este Estudio, se recogen:

- Automatización manejo de iluminación en exteriores (calles, etc.)
- Dispositivos, dispositivos virtuales y cosas (Tráfico)
- Servicio de compartición de bicicletas y coches
- Smart Parking
- Servicios de Información en áreas devastadas.

En revisiones del documento, actualmente en elaboración, se incluyen nuevos casos de usos como son por ejemplo el Riego inteligente.

Para cada uno de los Casos de uso se consideran los siguientes aspectos de interés:

- Descripción
- Actores
- Precondiciones
- Triggers
- Requisitos

6. ACRÓNIMOS

AEN/CTN	*Comité Técnico de Normalización de AENOR*
API	*Application Programming Interface*
ARIB	*Association of Radio Industries and Businesses*
ATIS	*Alliance for Telecommunications Industry Solutions*
CRM	*Customer Relationship Management*
ERP	*Enterprise Resource Planning*
ETSI	*European Telecommunications Standards Institute*
GIS	*Geographic Information System*
HMI	*Human Machine Interface*
HTTP	*Hypertext Transfer Protocol*
IOC	*Intelligent Operation Center*
iOS	*Sistema operativo de Apple*
IoT	*Internet of Things*
IT	*Information Technology*
JMX	*Java Management Extensions*
JSON	*JavaScript Object Notation*
M2M	*Machine to Machine communications*
MQTT	*Message Queue Telemetry Transport*
NGSI	*Next Generation Services Interface*
OIC	*Open Interconnect Consortium*
REST	*Representational State Transfer*
SCADA	*Supervisory Control And Data Acquisition*
SDK	*software development kit*
SETSI	*Secretaría de Estado de Telecomunicaciones y para la*
SOA	*Service-Oriented Architecture*
SNMP	*Simple Network Management Protocol*
TCP	*Transmission Control Protocol*
TIA	*Telecommunications Industry Association (North America)*

TIC	*Tecnologías de la información y la comunicación*
TR	*Technical report*
TS	*Technical specification*
TTA	*Telecommunications Technology Association (Korea)*
TTC	*Elecommunication Technology Committee (Japan)*
UNE	*Una Norma Española*
VEC	*Vehículo eléctrico conectado*
XML	*eXtensible Markup Language*

7. REFERENCIAS

[1] Interoperability best practices handbook. ETSI

[2] The interoperability enabler for the entire M2M and IOT ecosystem. White paper. oneM2M. January 2015

[3] http://iot.tid.es/iot/thinking-city/

[4] www.sofia2.com

[5] http://web01.abertis-telecom.preproduccion.com/es/productos/smartcities/productos/

[6] https://www.carriots.com/

[7] http://www.wonderware.es/

[8] http://www-03.ibm.com/software/products/es/intelligent-operations-center

[9] http://www.redbooks.ibm.com/redbooks/pdfs/sg248061.pdf

[10] UNE 178 104 Ciudades Inteligentes (AENOR). Infraestructuras. "Sistemas integrales de gestión de la Ciudad Inteligente"

[11] UNE 178 301 (AENOR). "Ciudades Inteligentes. Datos abiertos"

[12] TS-0001 (oneM2M). "Functional Architecture". V1.6.1

[13] TS-0002 (oneM2M). "Requirements" V1.0.1

[14] TR-0001 (oneM2M). "oneM2M Use Cases Collection" V0.0.5

[15] Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes. Red.es. PARTE 2: Metodología

[16] Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes. Red.es. PARTE 3: Cuestionarios

[17] Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes. Red.es. PARTE 4: Soluciones Alternativas

[18] http://www.agendadigital.gob.es/planes-actuaciones/Bibliotecaciudadesinteligentes/2.Materialcomplementario/normas_ciudades_inteligentes.pdf

Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes

PARTE 2: METODOLOGÍA Y ANÁLISIS

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO
ontsi observatorio nacional de las telecomunicaciones y de la SI

Este documento constituye una aproximación parcial al estudio de la interoperabilidad en nuestras ciudades; se enmarca dentro del *Servicio para el Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes* promovido por el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información, de Red.es, y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la información.

Para la realización de este estudio se ha contado con la colaboración de AT4 wireless S.A.U.

Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes

Año 2016

ÍNDICE

1. RESUMEN EJECUTIVO

La interoperabilidad es un elemento central en el desarrollo de las Ciudades Inteligentes. El Comité Técnico de Normalización AEN/CTN 178 "Ciudades inteligentes" movilizó un amplio consenso en la redacción de la norma: "Ciudades inteligentes. Infraestructuras. Sistemas Integrales de Gestión de la Ciudad Inteligente" (UNE 178 104)[12].

El presente estudio constituye una primera aproximación al conocimiento del concepto de interoperabilidad entre plataformas de gestión de servicios inteligentes. Se trata, por tanto, de un estudio parcial ya que está centrado en estándares que no tienen exactamente el mismo objeto, puesto que la Norma UNE 178 104 es más específica para la materia que el estándar oneM2M. Desde el Plan Nacional de Ciudades Inteligentes está previsto definir estudios que aborden con mayor profundidad los casos de aplicación que se consideren relevantes.

Este documento constituye la segunda de las cuatro partes que componen el informe de dicho estudio y recoge los resultados de la Fase 1 en la que se establece una comparativa entre los estándares de referencia (UNE 178 104 [12] y TS-0001 de oneM2M [14]); se define una metodología de análisis y cumplimiento de dichos requisitos; y en un documento aparte no publicable, se incluye un anexo confidencial donde se realiza un análisis de cumplimiento de las Plataformas participantes en este Estudio para los casos de uso identificados por oneM2M en el documento TR-001 [16] como son:

- Automatización manejo de iluminación en exteriores (calles, etc.)
- Servicio de compartición de bicicletas
- Smart Parking
- Gestión Semafórica.
- Riego inteligente

Para establecer la **comparativa**, ha sido necesario identificar los requisitos que se recogen en cada uno de los dos estándares de referencia [14][12], aplicados en particular a las Plataformas de Ciudad Inteligente.

Para ello, se han extraído los requisitos de ambas normas y posteriormente realizado una comparativa en forma de tabla entre ambos grupos de requisitos.

La conclusión final, es que ambos estándares son compatibles y complementarios de cara a garantizar la funcionalidad requerida, pero para tener la garantía de interoperabilidad es recomendable el cumplimiento de oneM2M por parte de las Plataformas, apps y dispositivos de Ciudades Inteligentes.

También se ha definido una **metodología formal de análisis y pruebas** de las Plataformas, abordándose tanto pruebas de Conformidad como de Interoperabilidad, pero centrándose principalmente en las pruebas de conformidad frente al documento UNE 178 104 [12] y la interoperabilidad con dispositivos, aplicaciones y Plataformas entre sí.

Dentro de este documento se incluye, como anexo de carácter confidencial, el análisis de cumplimiento de los casos de uso definidos por oneM2M para las Plataformas del Estudio, en base a un cuestionario que se ha proporcionado a las distintas empresas que disponen de este tipo de Plataformas en diferentes ciudades españolas y forman parte del Estudio:

- Thinking City de Telefónica [4]
- IOC de IBM [9]
- SmartBrain de Abertis (ahora Cellnex Telecom) [6]
- Sofia2 de Indra [5]
- Wonderware de Schenider-electric [8]
- Carriots de Wairbut [7]

Se han recibido respuestas formales al cuestionario por parte de todas las empresas consideradas.

La información proporcionada por cada una de ellas es desigual respecto a conceptos, contenidos y profundidad de la información. En el anexo se presenta el análisis de los Casos de uso en base a esa información recibida.

Es recomendable para siguientes análisis realizar entrevistas personales, una vez enviados los cuestionarios, con cada una de las empresas para aclarar conceptos y obtener un grado de información similar de todas ellas.

Las conclusiones más relevantes son las siguientes:

- El despliegue de los casos de uso incluidos en este Estudio no está integrado de manera masiva a través de las Plataformas en las ciudades españolas.

  Algunas entidades hacen referencia a otros casos de uso sí desplegados con las Plataformas de referencia, en la mayor parte de los casos a nivel de piloto, pero no hay muchos despliegues para los Casos de Uso que se plantean en el TR-0001 de oneM2M [16] para Ciudades Inteligentes.
- Respecto a los casos de uso seleccionados y analizados en este Estudio, no hay posibilidad directa de intercambio de sensores y servicios entre las diferentes Plataformas.

  Sí se pueden intercambiar, realizando pequeñas adaptaciones, entre aquellas Plataformas que comparten módulos específicos del proyecto FIWARE [3] como el Context Broker o IoTAgents. Para el intercambio con otras Plataformas es necesario realizar algún otro tipo de adaptación, principalmente en el modelo de datos.
- En el documento o Parte 4 de este Estudio se proponen medidas específicas de fomento del grado de interoperabilidad ofrecido por los dispositivos, aplicaciones y plataformas de un ecosistema de Ciudad Inteligente.

2. OBJETIVOS DEL DOCUMENTO

El objetivo final es buscar la portabilidad y reutilización de las aplicaciones y la compartición de dispositivos sobre las diferentes Plataformas de Gestión de Ciudades Inteligentes. Este estudio constituye una primera aproximación al conocimiento del concepto de interoperabilidad entre plataformas de gestión de servicios inteligentes. Desde el Plan Nacional de Ciudades Inteligentes está previsto definir estudios que aborden con mayor profundidad los casos de aplicación que se consideren relevantes.

Además se pretende conocer el posible impacto de la estandarización que se está llevando a cabo tanto a nivel nacional, en el CTN 178 de AENOR, como internacional, en el oneM2M, y sus posibles consecuencias en el desarrollo de soluciones Smart Cities en España, y tomar, a partir de las conclusiones de este Estudio, las medidas que se consideren oportunas.

Para ello, el Estudio se ha dividido en las siguientes fases:

- **E1: FASE 1**

1. **Identificación de puntos de referencia (o confluencia de estándares)** entre los que se puede establecer comparativa entre el modelo de capas propuesto en el documento UNE 178 104 [12] de AENOR y la arquitectura oneM2M [14].

2. Definición de una **metodología de análisis y cumplimiento de requisitos** para diferentes plataformas comerciales y casos de uso frente a los estándares de referencia.

3. **Analizar Casos de Uso** reales implantados en diferentes ciudades nacionales conforme establece oneM2M [16]. Los Casos de Uso seleccionados son:

    - Automatización manejo de iluminación en exteriores (calles, etc.)
    - Servicio de compartición de bicicletas
    - Smart Parking
    - Gestión Semafórica
    - Riego inteligente

- **E2: FASE 2**

Elaboración de **cuestionarios** de cumplimiento de requisitos frente a los estándares de referencia que permitan identificar diferentes grados de compatibilidad con los mismos.

- **E3: FASE 3**

  Propuesta de **soluciones interinas** que pudieran ser utilizadas para asegurar la interoperabilidad de las plataformas seleccionadas, en los casos de uso anteriores, minimizando en lo posible los costes de desarrollo, pero siempre admitiendo, a medio plazo, una evolución hacia los estándares propuestos en oneM2M.

Para completar el Estudio se han generado cuatro documentos, uno introductorio y otros tres correspondientes a cada una de las Fases definidas en el Estudio. Este documento constituye el resultado de la Fase 1 del Estudio.

El objetivo de este documento es triple:

- Realizar una comparativa de estándares a nivel de requisitos,
- Definir una metodología formal para verificar el cumplimiento de los requisitos por parte de las Plataformas de Ciudad Inteligente,
- Analizar los casos de uso sobre sistemas implantados usando las Plataformas incluidas en el Estudio.

3. CONFLUENCIA DE ESTÁNDARES

El objetivo de este apartado es establecer la comparativa entre el modelo de capas propuesto en el documento UNE 178 104 [12], y la arquitectura TS-0001 [14] del Comité oneM2M.

Por un lado, el documento UNE 178 104 es específico para las Plataformas de gestión de ciudad inteligente, mientras que la especificación técnica TS-0001 contempla todos los elementos que forman parte de un ecosistema IoT, tanto plataformas como aplicaciones, dispositivos y gateways.

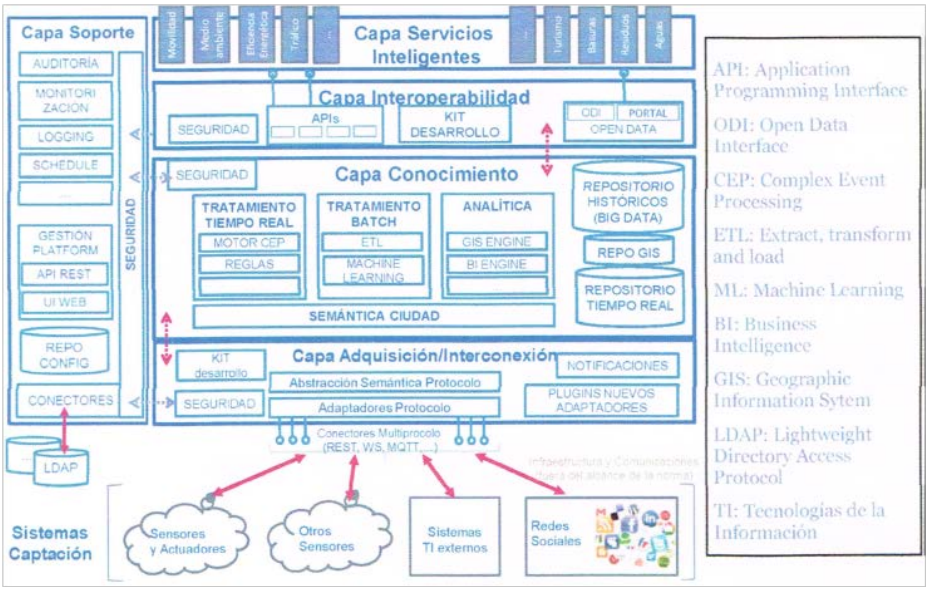
Para establecer una comparativa, es necesario, por tanto, definir los requisitos que se recogen en cada uno de los estándares, aplicados en particular a las Plataformas de Gestión de Ciudad Inteligente.

Para ello se han extraído los **requisitos de ambas normas y posteriormente realizado una comparativa** en forma de tabla entre ambos grupos de requisitos.

Como punto de partida, las **Plataformas de Gestión de Ciudad Inteligente**, referenciadas en el documento de AENOR, se corresponden con lo que se denomina **Nodos de infraestructura (IN)** en la especificación TS-0001 [14], por lo que principalmente esta comparativa se ha focalizado en los requisitos que se definen en la especificación para este tipo de nodos.

A continuación se presenta un pequeño resumen de lo recogido en el documento de Síntesis de la situación de partida que permitirá un mejor seguimiento de este documento.

El esquema de arquitectura de capas de la norma UNE [12] es el siguiente:



Donde:

Sistemas de captación: Lo forman las redes de sensores y actuadores, sistemas externos, redes sociales, etc.

Capa de adquisición/interconexión: Ofrece los mecanismos para la captación de datos desde los sistemas de captación y abstrae la información con un enfoque semántico estándar.

Capa de conocimiento: Recibe datos de las capas de adquisición e interoperabilidad y ofrece el procesado de datos, la incorporación de valor y la transformación de servicio.

Capa de interoperabilidad: Ofrece interfaces y conectores para que los sistemas externos puedan acceder a la plataforma y permite construir servicios a partir de los datos. Para ello, debe ofrecer la API nativa de acceso a los datos de la capa de conocimiento.

Capa de servicios inteligentes: Está constituida por los servicios municipales conectados a través de la capa de interoperabilidad. Estos servicios pueden formar parte de la Plataforma o ser externos.

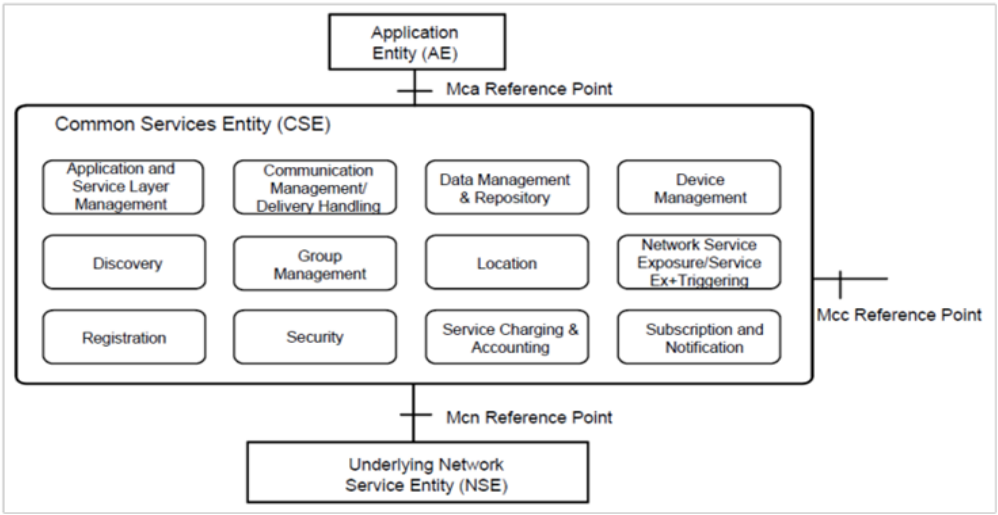
Capa de soporte: Ofrece servicios comunes como auditoria, monitorización, seguridad, etc…

Los **puntos de referencia**, similares a los establecidos en la TS-0001 [14], son las interfaces que presenta la arquitectura para interactuación con:

1. Otras aplicaciones o servicios de terceros a través de la capa de interoperabilidad,
2. Otras aplicaciones o servicios de terceros a través de la capa de adquisición o interconexión,
3. Dispositivos o gateways a través de la capa de adquisición o interconexión
4. Entre servicios comunes de la Plataforma en las capas de soporte y conocimiento y de estas con el resto de capas.

Este estudio se ha centrado principalmente en las tres primeras interfaces o puntos de referencia y los requisitos asociados a cada una de ellos, además de en los servicios comunes exigidos que debe incluir una Plataforma de gestión de Ciudad Inteligente según el documento UNE 178 104 [14].

El esquema funcional equivalente de la especificación TS-0001 [14] es:



Donde

AE (Application Entity): Es una entidad en la capa de aplicación que implementa la lógica de servicio de una aplicación M2M y tiene un único identificador AE-ID. Algunos ejemplos pueden ser: aplicación de gestión de flotas, aplicación de monitorización remota de la glucosa, aplicación de medida de consumo, etc.

CSE (Common Services Entity): Es una entidad que representa una instancia de un conjunto de funciones de servicios comunes en el entorno M2M y están identificadas unívocamente como CSE-ID. Estos servicios comunes son ofrecidos al resto de entidades. Algunos ejemplos son: gestión de datos, gestión de dispositivos a nivel de servicio, gestión de subscripciones o servicios de localización.

NSE (Network Service Entity): Ofrece servicios desde la red subyacente a los CSE. Algunos ejemplos son: gestión de dispositivos a nivel de red o triggering de dispositivos.

Los **puntos de referencia** en este caso son: Mcn, Mcc y Mca.

3.1. REQUISITOS FUNCIONALES DE UNE 178 104

Aplicando la metodología de extracción de requisitos sobre el documento UNE 178 104 [12], se han identificado los siguientes.

3.1.1. REQUISITOS FUNCIONALES

Repositorio de información

ID	DESCRIPCIÓN
REP-001	La plataforma debe albergar un catálogo común, universal, mantenido, accesible y clasificado de datos únicos y normalizados de la ciudad.
	La plataforma debe albergar un catálogo también de datos sobre los

REP-002	activos, ya que la gestión de los mismos es cada vez más relevante en los proyectos de Smart Cities. La normalización de la nomenclatura a utilizar para los activos así como la información requerida dependiendo del tipo que sea cada uno de ellos, es muy importante para que las aplicaciones de gestión de los mismos los reconozcan y se garantice la interoperabilidad.
REP-003	La plataforma debe permitir visiones analíticas transversales de la ciudad a partir de estos datos.
REP-004	La plataforma debe facilitar y universalizar la integración de datos de alta y baja latencia y del legacy de soluciones existentes en la ciudad.
REP-005	La plataforma debe explotar los datos de Ciudad y ofrecer las interfaces para el desarrollo de aplicaciones Smart a partir de ellos, conforme a permisos de acceso a la información adecuados a cada actor específico.

Gestión de infraestructuras

ID	DESCRIPCIÓN
INFR-001	Debe soportar acceso a los datos de plataformas de sensores, bases de datos y a información de otras aplicaciones.
INFR-002	La plataforma debe permitir actuaciones sobre actuadores (sensores) a través de soluciones estandarizadas.
INFR-003	La plataforma debe soportar el registro de las diferentes actividades que se desarrollan en el sistema.
INFR-004	La plataforma debe soportar la gestión del mantenimiento de equipos e infraestructuras.
INFR-005	La plataforma debe soportar protocolos estándar de monitorización como SNMP y JMX.
INFR-006	La plataforma debe permitir la integración con otros sistemas y aplicaciones.

Comunicación entre sistemas (Interoperabilidad)

ID	DESCRIPCIÓN
INT-001	La plataforma debe proveer las interfaces necesarias para que eventos de un sistema puedan desencadenar acciones en otros.
INT-002	La plataforma debe usar APIs y protocolos normalizados para la comunicación entre aplicaciones.
INT-003	La plataforma debe tener la capacidad de extenderse para

	soportar otros protocolos de comunicación con sensores.

Seguridad

ID	DESCRIPCIÓN
SEC-001	La plataforma debe soportar autenticación y autorización.
SEC-002	La plataforma debe controlar el acceso a la plataforma y a todos los elementos a los que se acceda a través de esta: sensores, scadas, centros de control, bases de datos y aplicaciones.
SEC-003	La plataforma debe garantizar confidencialidad en la comunicación con la Plataforma
SEC-004	La plataforma debe garantizar confidencialidad en el acceso a los datos, de modo que cada rol sólo pueda ver los datos a los que tiene acceso.
SEC-005	La plataforma debe definir y gestionar políticas de seguridad.
SEC-006	La plataforma debe proveer un módulo central y de fácil acceso (vía web) para poder realizar gestiones de administración de los usuarios, roles y permisos.
SEC-007	La plataforma debe soportar diferentes mecanismos de autenticación como soluciones basadas en usuario y contraseña en tokens, en OAuth, en certificados electrónicos (de individuos, servidores y aplicaciones) u otro tipo de soluciones avanzadas basadas, por ejemplo, en técnicas biométricas.
SEC-008	La plataforma debe permitir la integración con repositorio de usuarios ya existentes en la AAPP, del estilo LDAP, Base de Datos de usuarios, etc.
SEC-009	La plataforma debe tener capacidad de extenderse para adaptar los mecanismos de seguridad a las necesidades propias de cada ciudad.
SEC-010	La plataforma debe asegurar la privacidad y seguridad de los datos almacenados o gestionados por la solución, especialmente en un entorno compartido de recursos (PaaS: Plataforma como Servicio). Asimismo, se deben poder definir distintos perfiles de acceso a los diferentes tipos/grupos de datos, que eviten un uso inadecuado de los mismos.
SEC-011	La plataforma debe garantizar el envío y recepción segura de datos desde y hacia los dispositivos conectados a ella, así como su distribución segura a los aplicativos que los requieran. Como

	mínimo debe implementar la autenticación de los elementos que originan los datos y de los aplicativos que requieren acceso a dichos datos.
SEC-012	La plataforma debe permitir definir diferentes roles y niveles de acceso sobre los datos, funcionalidades y servicios de la plataforma, autorizar o denegar el acceso a los distintos aplicativos y definir los privilegios requeridos para actuar sobre un determinado conjunto de datos. Los usuarios de la Plataforma Integrada pueden ser individuos o aplicaciones que consuman servicios o información. Hay que considerar diferentes tipos de acceso: usuario de la plataforma (persona a través de consola o web, aplicaciones a través de los servicios y APIs), usuarios internos, terceros, de confianza, etc, con diferentes roles: - Administrador del sistema. - Operador - Directivos - Clientes sw de otras aplicaciones - etc. La gestión de roles/permisos se establecerá como mínimo respecto a tres niveles de seguridad: a. Acceso a los datos: limitar la información que puede visualizar cada usuario. Por ejemplo: a un usuario de un determinado Servicio sólo tendrá acceso a la información correspondiente a los datos de su Servicio, datos generales como medidas globales, desviaciones y otros que se obtengan del tratamiento conjunto de los datos correspondientes a todos los Servicios. b. Acceso a los elementos de la Plataforma Integral: limitar el acceso a los informes y cuadro de mando configurados en la Plataforma Integral Por ejemplo un usuario de un Servicio sólo podrá acceder a los informes definidos con los datos correspondiente a su ámbito c. Funcionalidad: delimitar las acciones que puede realizar un determinado usuario en función de su perfil

Mantenimiento

ID	DESCRIPCIÓN
MANT-001	La plataforma debe facilitar el almacenamiento y valoración de indicadores relevantes para la gestión del mantenimiento.
MANT-002	La plataforma debe facilitar la generación de planes de mantenimiento a partir de indicadores relevantes para la gestión del mantenimiento.

MANT-003	La plataforma debe permitir la posibilidad de gestionar los avisos o alarmas y poder enviar mensajes, correos, SMS y llamadas en función de indicadores relevantes para la gestión del mantenimiento.
MANT-004	La plataforma debe permitir la posibilidad de integración nativa con sistemas móviles y apps.

Desarrollo de aplicaciones

ID	DESCRIPCIÓN
APP-001	La plataforma debe permitir realizar análisis de consumos, alarmas, tendencias, etc.
APP-002	La plataforma debe permitir realizar imputación de costes.
APP-003	La plataforma debe permitir realizar optimización de procesos y planificación.
APP-004	La plataforma debe permitir realizar un control de calidad de servicios públicos por terceros.
APP-005	La plataforma debe permitir realizar una sala de crisis.
APP-006	La plataforma debe soportar la generación de informes de explotación.
APP-007	La plataforma debe poder integrarse con herramientas para el análisis de todos estos indicadores.

Soporte a la decisión

ID	DESCRIPCIÓN
DSS-001	La plataforma debe integrar herramientas de simulación en base a la información actual e histórica.
DSS-002	La plataforma debe integrar herramientas de valoración y ejecución de planes de actuación, en escenarios complejos.
DSS-003	La plataforma debe integrar herramientas de análisis predictivo y modelado de la ciudad.
DSS-004	La plataforma debe integrar herramientas de minería de datos y el análisis estadístico.
DSS-005	La plataforma debe integrar herramientas de integración con otros sistemas y herramientas Business Intelligence.

Publicación de información

ID	DESCRIPCIÓN
PUBL-001	La plataforma debe permitir transmitir información abierta y en formatos estándar.
PUBL-002	La plataforma debe permitir transmitir información accesible a multidispositivos.
PUBL-003	La plataforma debe permitir transmitir información de forma continua y sin interrupciones.
PUBL-004	La plataforma debe permitir transmitir información aplicable a servicios finalistas al ciudadano (sociedad de la información).
PUBL-005	La plataforma debe permitir transmitir información aplicable a aplicaciones de terceros (open data).
PUBL-006	La plataforma debe permitir transmitir información aplicable a otros servicios públicos y administraciones.
PUBL-007	La plataforma debe permitir transmitir información aplicable a rendición de cuentas (transparencia).

Resistencia a fallos

ID	DESCRIPCIÓN
FALL-001	La plataforma debe garantizar la continuidad operativa de los servicios inteligentes de acuerdo con los niveles de servicios contratados. Estos servicios podrían requerir disponibilidad 24x7 y un nivel de servicio superior al 99.9% anual y se incluirán en las métricas. El proveedor deberá ofrecer soluciones que garanticen funcionamiento ante cualquier incidente o emergencia, necesarias para cumplir este requisito.
FALL-002	La plataforma debe garantizar la recuperación en caso de desastres como un RTO (Objetivo de Tiempo de Recuperación) y un RPO (Objetivo de Punto de Recuperación) limitados, que se valorarán en las métricas.

3.1.2. REQUISITOS TÉCNICOS

ID	DESCRIPCIÓN
RTEC-001	Horizontalidad: capacidad de soporte de diferentes ámbitos de aplicación, de manera que sea posible la implementación

	simultánea de múltiples servicios en la misma infraestructura.
RTEC-002	Interoperabilidad: capacidad de soporte de diferentes tecnologías, dispositivos y mecanismos de captura de información, y estándares de comunicación, así como otros sistemas de información internos/corporativos y/o externos.
RTEC-003	Rendimiento: habilidad del sistema para manejar en tiempo real un elevado número de dispositivos, servicios y procesos de manera eficiente.
RTEC-004	Escalabilidad: capacidad de poder incrementar capacidad de proceso y almacenamiento sin tener que modificar la arquitectura.
RTEC-005	Robustez y Resiliencia: capacidad para seguir funcionando ante problemas.
RTEC-006	Modularidad: la plataforma debe tener un enfoque modular que permita desplegarla por partes (por ejemplo, módulo Big Data) de forma sencilla.
RTEC-007	Continuidad operativa o disponibilidad: capacidad del sistema para estar operativo en cualquier momento.
RTEC-008	Capacidad de Recuperación: capacidad para gestionar de forma eficiente los fallos que puedan afectar a la disponibilidad.
RTEC-009	Flexibilidad: habilidad de la plataforma para funcionar con diferentes servicio inteligentes de ciudad.
RTEC-010	Extensibilidad: capacidad de la plataforma para poder ampliarse para dar soporte a nuevas necesidades.
RTEC-011	Capacidades Big Data: capacidad para integrar una gran cantidad de datos generados desde múltiples fuentes y con diferentes estructuras.
RTEC-012	Basada en estándares abiertos: lo que simplifica la integración con otras plataformas y el desarrollo de aplicaciones sobre la Plataforma que puedan ser reusables y portables entre diferentes plataformas.
RTEC-013	Evolucionable: facilitando su capacidad de extensión en el futuro mediante estándares ampliamente adoptados.
RTEC-014	Integral: la plataforma debe trabajar como un todo, no como piezas desacopladas que no están preparadas para trabajar en conjunto.
RTEC-015	Operable y gestionable: la plataforma debe poder gestionar, operar, mantener e instalarse de forma sencilla.
RTEC-016	Semántica: el uso de conceptos semánticos en la Plataforma

	permite la interoperabilidad entre plataformas y por tanto entre ciudades.
RTEC-017	Seguridad: garantía del sistema en cuanto a seguridad, privacidad y confianza se refiere.

3.1.3. ARQUITECTURA DE CAPAS

ID	DESCRIPCIÓN
ARQ-001	La plataforma se ajusta al sistema de capas propuesto en el documento.

Capa de adquisición / Interconexión

ID	DESCRIPCIÓN
ADQ-001	Independencia del operador de red.
ADQ-002	Integración de la información desde las fuentes de datos (sensores, dispositivos etc.).
ADQ-003	Suministrar la información a la capa de conocimiento con independencia de los dispositivos dando una vista semántica de los datos adquiridos.
ADQ-004	Se debe adaptar al modelo ETSI M2M. Tener interfaces abiertos y estandarizados sobre los que será posible desarrollar aplicaciones de terceros que interactúen directamente con los dispositivos, no propietarios.
ADQ-005	Solución de capa de adquisición única para distintos servicios.
ADQ-006	Independencia de la tecnología de acceso y sensores.
ADQ-007	Posibilidad de añadir nuevos conectores.
ADQ-008	Acceso a los sensores.
ADQ-009	Modulo capaz de conectar escenarios compatibles con oneM2M.

Capa de conocimiento

ID	DESCRIPCIÓN
CON-001	Acceso a toda la información tanto histórica como en tiempo real.
CON-002	Movimiento de datos recibidos por la capa de adquisición para

	almacenamiento, proceso y recuperación y a disposición de la capa de interoperabilidad siguiendo modelos de datos.
CON-003	Soporte tratamiento en tiempo real de los datos recibidos de la capa de adquisición a través de motor de reglas, etc.
CON-004	Soporte en tratamiento Batch de los datos recibidos a través de ETL ("Extraer, transformar y cargar").
CON-005	Soporte tratamiento analítico de los datos mediante procesos Business Intelligence.
CON-006	Soporte tratamiento GIS, permitiendo georeferencias de datos y hacer consultas geográficas.
CON-007	Seguridad: se controla usuario/rol para cada dato.
CON-008	Aplicar semánticas creadas por organizaciones internacionales o crearlas si no existen vocabularios y publicarlos.

Capa de Interoperabilidad

ID	DESCRIPCIÓN
CIN-001	Publicación de APIs que garanticen la portabilidad de aplicaciones entre ciudades y plataformas, debe ser de tipo REST con diferentes modos de acceso (Incluyendo modo Push y Pull) así como consultas georeferenciadas.
CIN-002	Capacidad de interconexión con aplicaciones y plataformas.
CIN-003	Acceso a servicios externos.
CIN-004	Publicación de un portal opendata.
CIN-005	Kit de desarrollo con SDK y APIs para construir servicios.
CIN-006	Modelo de acceso a datos agnóstico. Se recomienda el modelo oneM2M.

Capa de Servicios Inteligentes

ID	DESCRIPCIÓN
SER-001	Centro de mandos personalizados e indicadores para diferentes ubicaciones de despliegue en función del perfil y de los permisos del usuario.
SER-002	Aplicaciones de gestión de los servicios verticales.

SER-003	Aplicaciones de gestión de los contratos (SLA en bases de datos).

Capa de Soporte

ID	DESCRIPCIÓN
SOP-001	Entorno Web de Gestión de la configuración permitiendo a través de una aplicación Web de gestión de toda esta, incluyendo interfaces REST de gestión.
SOP-002	Repositorio de configuración de la plataforma de modo que exista un lugar centralizado de almacenamiento de toda esta.
SOP-003	Seguridad de acceso (Usuario y que rol tiene para acceder a los datos) y Conectores de Repositorio de Seguridad de modo que la seguridad pueda delegarse al gestor de usuarios de la ciudad.

3.1.4. INTEROPERABILIDAD ENTRE PLATAFORMAS

ID	DESCRIPCIÓN
IPL-001	Independencia en el dominio de las apps.
IPL-002	Independencia en el dominio de la red.
IPL-003	Independencia en el dominio del sistema de adquisición.

3.2. REQUISITOS FUNCIONALES DE TS-0001

El documento “TS-0002 Requirement” [15] del oneM2M contiene los requisitos técnicos que se listan a continuación.

3.2.1. REQUISITOS GENERALES

ID	DESCRIPCIÓN
OSR-001	El sistema oneM2M debe permitir comunicación entre aplicaciones M2M usando múltiples medios de comunicación basados en acceso mediante IP.
OSR-002a	El sistema oneM2M debe permitir medios de comunicación con dispositivos con capacidades reducidas de computación (ej. CPU, memoria o batería reducidas) o de comunicación (ej. modem inalámbrico 2G).
OSR-	El sistema oneM2M debe permitir medios de comunicación con

002b	dispositivos con elevadas capacidades de computación (ej. CPU, memoria o batería de complejidad avanzada) o de comunicación (ej. modem inalámbrico 3G).
OSR-003	El sistema oneM2M debe soportar comunicaciones entre aplicaciones (A2A) en coordinación con una sesión de aplicación para las aplicaciones M2M que lo requieran.
OSR-004	El sistema oneM2M debe soportar comunicaciones entre aplicaciones sin establecimiento de sesión para las aplicaciones M2M que lo requieran.
OSR-005	El sistema oneM2M debe ser capaz de descubrir los servicios ofrecidos por redes de comunicación a aplicaciones M2M (ej. SMS, USSD, localización, configuración de suscripción, autenticación, etc.), sujetos a las reglas de restricciones del correspondiente operador de red.
OSR-006	El sistema oneM2M debe ser capaz de reutilizar servicios ofrecidos por las redes subyacentes a aplicaciones/servicios M2M ,a través de modelos de acceso abiertos (ej. OMA, framework GSMA OneAPI). Algunos ejemplos de servicios disponibles son: • Comunicaciones IP multimedia. • Mensajería • Localización. • Servicios de tarificación y facturación. • Información de dispositivos y perfiles. • Configuración y gestión de dispositivos. • Activación y monitorización de dispositivos. • Pequeñas transmisiones de datos. • Gestión de grupos.
OSR-007	El sistema oneM2M debe proveer un mecanismo para que las aplicaciones M2M interactúen con las aplicaciones y con los datos/información gestionados por un proveedor de servicio M2M diferente, sujeto a los permisos apropiados.
OSR-008	El sistema oneM2M debe proveer la capacidad para que aplicaciones M2M se comuniquen con dispositivos M2M (ej. una aplicación en un dispositivo), sin la necesidad de conocer la tecnología o el protocolo de comunicación específico de dichos dispositivos M2M.
OSR-009	El sistema oneM2M debe soportar la capacidad de que una o múltiples aplicaciones M2M interactúen con uno o múltiples dispositivos/gateways M2M (aplicación en el dispositivo/gateway).
OSR-010	El sistema oneM2M debe soportar mecanismos de confirmación de la correcta entrega de mensajes a su destino, a aquellas aplicaciones M2M que requieran un envío confiable para detectar fallos en mensajes en un intervalo de tiempo dado.
OSR-011a	El sistema oneM2M debe ser capaz de solicitar diferentes caminos de comunicación de la red subyacente, basándose en las reglas del

	proveedor de servicios M2M o del operador de red, con mecanismos de enrutamiento para evitar fallos en la transmisión.
OSR-011b	El sistema oneM2M debe ser capaz de solicitar diferentes caminos de comunicación de la red subyacente según las peticiones de las aplicaciones M2M
OSR-012	El sistema oneM2M debe soportar comunicaciones entre aplicaciones M2M y dispositivos soportando servicios M2M por medio de una conectividad continua o no-continua.
OSR-013	El sistema oneM2M debe conocer la tolerancia de retardo aceptable por la aplicación M2M y debe programar la comunicación o pedir a la red subyacente que lo haga, según del criterio de reglas definido.
OSR-014	El sistema oneM2M debe ser capaz de comunicarse con dispositivos M2M, conectados a través de un Gateway M2M capaz de soportar redes M2M heterogéneas.
OSR-015	El sistema oneM2M debe ser capaz de ayudar a las redes subyacentes que soportan diferentes esquemas de comunicación, incluyendo comunicaciones poco frecuentes, transferencia de pequeñas cantidades de datos, transferencia de grandes archivos y comunicaciones en modo streaming.
OSR-016	El sistema oneM2M debe proveer la capacidad de notificar a aplicaciones M2M de la disponibilidad, o cambios, de aplicaciones o información de gestión de un dispositivo/gateway M2M disponible, incluyendo cambios en la red M2M.
OSR-017	El sistema oneM2M debe ser capaz de ofrecer acceso a diferentes tipos de servicios M2M a los proveedores de servicios M2M. Estos servicios han de incluir, como mínimo: • Gestión de la conectividad. • Gestión de dispositivos (a nivel de servicio). • Gestión de datos de aplicación. Para permitir distintos escenarios de desarrollo, estos servicios han de ser ofrecidos por el sistema oneM2M, individualmente, como un subconjunto o un conjunto completo de servicios.
OSR-018	El sistema oneM2M debe ser capaz de ofrecer servicios M2M a dispositivos M2M en itinerancia a través las redes celulares subyacentes, según restricciones basadas en las reglas del operador de red.
OSR-019	El sistema oneM2M debe soportar la capacidad de repositorio de datos (ej. recopilación/almacenamiento) y de transferencia de datos desde uno o más dispositivos/gateways M2M hacia uno o más gateways M2M, infraestructuras de servicios M2M o infraestructuras de aplicaciones M2M, de la forma requerida por la infraestructura de aplicación M2M como se muestra debajo: • Acción iniciada tanto por un dispositivo M2M, un gateway

	M2M, infraestructuras de servicios M2M o infraestructuras de aplicaciones M2M. • Iniciada por un evento o una activación programada. • Para datos específicos.
OSR-020	El sistema oneM2M debe admitir reglas sobre los aspectos de almacenamiento y recuperación de datos/información, así como gestión de las mismas.
OSR-021	El sistema oneM2M debe proveer mecanismos para permitir la compartición de datos entre múltiples aplicaciones M2M.
OSR-022	Cuando algunos de los componentes de una solución oneM2M no estén disponibles (ej. Conexión WAN pérdida), el sistema oneM2M deberá permitir el correcto funcionamiento del resto de componentes disponibles de dicha solución oneM2M.
OSR-023	El sistema oneM2M debe ser capaz de identificar los servicios M2M a usar por parte de las diferentes suscripciones de Servicio M2M.
OSR-024	El sistema oneM2M debe ser capaz de identificar los dispositivos M2M a usar por parte de las diferentes suscripciones de Servicio M2M.
OSR-025	El sistema oneM2M debe ser capaz de identificar las aplicaciones M2M a usar por parte de las diferentes suscripciones de Servicio M2M.
OSR-026	El sistema oneM2M debe poder asociar los dispositivos M2M usados por las suscripciones de Servicio M2M con los identificadores de dispositivo ofrecidos por la red subyacente y el dispositivo, siempre que la red subyacente lo permita.
OSR-027	El sistema M2M debe proveer un mecanismo genérico para permitir el intercambio transparente de datos entre la aplicación M2M y la red subyacente, sujeto a las restricciones basadas en la política del proveedor de servicios M2M y/o en la del operador de red.
OSR-028	El sistema oneM2M debe permitir a una aplicación M2M definir condiciones de activación en el sistema, tales que éste pueda enviar de forma autónoma comandos a actuadores en nombre de la aplicación M2M cuando las mencionadas condiciones se cumplan.
OSR-029	El sistema oneM2M debe poder enviar comandos comunes a varios actuadores o sensores a través de un grupo.
OSR-030	El sistema oneM2M permitir la gestión (ej. Añadir, borrar, modificar y obtener) de los miembros de un grupo.
OSR-031	El sistema oneM2M debe permitir a un grupo ser un miembro de otro grupo.
OSR-032	El sistema oneM2M debe permitir distintas categorías de evento (ej. normal, urgente) asociadas a la recepción, almacenado o reporte de datos por parte de una aplicación M2M.

OSR-033	El sistema oneM2M debe proveer la capacidad de ajustar dinámicamente la programación de informes y notificaciones de un dispositivo/gateway M2M, basándose en el contexto de dispositivos/gateways dinámicos del dispositivo/gateway M2M y en las categorías de eventos previamente definidas.
OSR-034	El sistema oneM2M debe permitir el reemplazo sin interrupción de dispositivos M2M así como de gateways M2M (ej. redirección de tráfico, conexión, recuperación, etc.).
OSR-035	El sistema oneM2M debe permitir el intercambio de información relevante de aplicaciones no-M2M (ej. Clases de dispositivos/gateways) con dispositivos/gateways M2M e infraestructuras de servicios M2M con el propósito de facilitar una comunicación eficiente. Esto incluye la capacidad de que un dispositivo M2M informe de su clase de dispositivo a la infraestructura de servicio M2M y de que la infraestructura de servicio M2M informe de sus capacidades al dispositivo M2M.
OSR-036	El sistema oneM2M debe proveer mecanismos para aceptar peticiones de aplicaciones proveedoras de servicios M2M para realizar servicios de analítica.
OSR-037	El sistema oneM2M debe permitir a cualquier aplicación M2M solicitar el envío de datos, de forma independiente de la red subyacente, a las aplicaciones M2M de un grupo de dispositivos y gateways M2M, en zonas geográficas especificadas por la aplicación M2M.
OSR-038	El sistema oneM2M debe soportar la inclusión de preferencias de calidad de servicio (QoS) de aplicaciones M2M en peticiones de servicio a la red subyacente.
OSR-039	El sistema oneM2M debe poder autorizar peticiones de servicio con preferencias QoS a nivel de servicio, pero las preferencias de QoS de aplicaciones M2M deben ser pasadas a las redes subyacentes en las solicitudes de servicio, para llevar a cabo la autorización y concesión o negociación de las peticiones de QoS de servicio.
OSR-040	El sistema oneM2M debe poder hacer uso de múltiples mecanismos de comunicación (tales como USSD o SMS) cuando estén disponibles en las redes subyacentes.
OSR-041	El sistema oneM2M debe proveer un mecanismo que soporte la inclusión de nuevos servicios M2M en un sistema oneM2M, implementados como módulos transferibles independientes por medio de las interfaces de oneM2M.
OSR-042	El sistema oneM2M debe soportar diferentes niveles de QoS, identificando parámetros tales como la tasa de bit garantizada, retardo, variaciones de retardo, tasa de pérdidas y tasa de error, etc.
OSR-043	El sistema oneM2M debe poder verificar que miembros de un grupo soportan un conjunto de funciones comunes.

OSR-044	El sistema oneM2M debe soportar comunicación tanto con dispositivos M2M que son accesibles de forma programada (ej. periódica), como también con dispositivos M2M que son accesibles de una forma espontánea e impredecible.
OSR-045a	El sistema oneM2M debe poder recibir y utilizar información obtenida de la red subyacente sobre cuándo un dispositivo M2M puede ser accedido.
OSR-045b	El sistema oneM2M debe poder utilizar programaciones de accesibilidad generados tanto por el dispositivo M2M como por el Dominio de la Infraestructura.
OSR-046	El sistema oneM2M debe soportar la capacidad de que una aplicación M2M pueda requerir o rechazar confirmación para sus comunicaciones.
OSR-047	El sistema oneM2M debe soportar mecanismos para que los dispositivos M2M y/o Gateways informen sobre su localización geográfica a aplicaciones M2M.
OSR-048	El sistema oneM2M debe proveer un servicio M2M que permita a dispositivos M2M y/o gateways compartir su información de localización geográfica o la de otros dispositivos M2M
OSR-049	El sistema oneM2M debe proveer la capacidad para que una aplicación M2M pueda compartir datos entre Aplicaciones de forma selectiva.
OSR-050	Si la comunicación mediante un canal proporcionado por la red subyacente solo puede ser activada unidireccionalmente (Dominio de campo o dominio de infraestructura), y hay canales alternativos disponibles en la otra dirección, el sistema oneM2M debe poder usar estos canales alternativos para activar la comunicación bidireccional en el primer canal.
OSR-051	Dependiendo de la disponibilidad de interfaces apropiados proporcionados por la red subyacente, el sistema oneM2M debe poder pedir a la red que retransmita datos en modo difusión/multidifusión a un grupo de dispositivos M2M en un área específica.
OSR-052	El sistema oneM2M debe poder seleccionar una red apropiada para la difusión/multidifusión de datos, dependiendo de las capacidades de la red y la conectividad soportada por el grupo seleccionado de dispositivos/gateways M2M.
OSR-053	El sistema oneM2M debe proveer un medio que permita la compatibilidad hacia atrás de interfaces entre diferentes versiones.
OSR-054	El sistema oneM2M debe permitir que una aplicación, un dispositivo, o un gateway M2M obtengan acceso a los recursos de otra aplicación, dispositivo o gateway M2M.
OSR-055	El sistema oneM2M debe proveer la capacidad de que las aplicaciones

	M2M intercambien datos con una o más aplicaciones M2M que no sean conocidas de antemano.
OSR-056	El sistema oneM2M debe permitir el descubrimiento de aplicaciones M2M utilizables, en un gateway o dispositivo M2M.
OSR-057	El sistema oneM2M debe permitir el descubrimiento de gateways y dispositivos M2M disponibles a una aplicación M2M para el intercambio de datos.
OSR-058	El sistema oneM2M debe proveer marcas de tiempo según sea necesario para las funciones de servicios comunes.
OSR-059	El sistema oneM2M debe ser capaz de permitir control de acceso basado en roles según las suscripciones a servicios M2M.
OSR-060	El sistema oneM2M debe permitir la sincronización temporal con un reloj externo.
OSR-061	Los dispositivos y gateways M2M pueden soportar sincronización temporal conforme al sistema oneM2M.
OSR-062	El sistema oneM2M debe permitir medios para la comprobación de la conectividad entre un conjunto de aplicaciones M2M.
OSR-063	El sistema oneM2M debe poder gestionar la planificación de la conectividad y mensajería de la capa de servicio M2M entre el dominio de infraestructura y los dispositivos/gateways M2M.
OSR-064	El sistema oneM2M debe poder agrupar mensajes dependiendo de la tolerancia al retardo del mensaje y/o su categoría.
OSR-065	El sistema oneM2M debe proporciona mecanismos que permitan a un proveedor de servicios M2M distribuir funciones de procesado a sus dispositivos/gateways M2M en el dominio de campo.
OSR-066	El sistema oneM2M debe permitir la colocación y operación de aplicaciones M2M en nodos M2M seleccionados según criterios requeridos por los proveedores de servicios de aplicación, sujeto a los derechos de acceso.
OSR-067	El sistema oneM2M debe ser capaz de tomar acciones operacionales y de gestión, según lo requerido por las aplicaciones M2M.
OSR-068	Cuando esté disponible en la red subyacente, el sistema oneM2M proveerá la capacidad de obtener y presentar información acerca de si un dispositivo M2M está autorizado a acceder a los servicios de la red subyacente.
OSR-069	Cuando esté disponible en una red, el sistema oneM2M mantendrá el estado operacional del servicio M2M de un dispositivo M2M y lo actualizará cuando el estado del servicio de conectividad de la red subyacente cambie.

OSR-070	El sistema oneM2M debe proveer la capacidad de notificar a una aplicación M2M autorizada sobre cuándo el estado administrativo u operacional del servicio M2M de un dispositivo M2M cambie, siempre que esa aplicación M2M esté suscrita a tales notificaciones.
OSR-071	El sistema oneM2M debe permitir a una aplicación M2M autorizada cambiar el estado administrativo de un servicio M2M en un dispositivo M2M.
OSR-072	El sistema oneM2M debe poder iniciar un conjunto de acciones bien definidas (ej. activación si sobrepasa un umbral, comparar un valor, etc.) en una o más aplicaciones M2M en nombre de otra aplicación M2M.

En la versión borrador de este documento [15] se están discutiendo requisitos adicionales que no serán tenidos en consideración por no estar consensuados a la fecha de este informe.

3.2.2. REQUISITOS DE GESTIÓN

ID	DESCRIPCIÓN
MGR-001	El sistema oneM2M podrá soportar la gestión y la configuración de dispositivos/gateways M2M incluyendo dispositivosM2M con recursos limitados.
MGR-002	El sistema oneM2M será capaz de descubrir redes M2M, incluyendo información sobre sus dispositivos y los parámetros de dichas redes (ej. topología, protocolo).
MGR-003	El sistema oneM2M será capaz de proveer la capacidad de mantener y describir el modelo de información de gestión de los dispositivos y parámetros (ej. topología, protocolo) de redes M2M.
MGR-004	El sistema oneM2M soportará mecanismos comunes de gestión de dispositivos mediante diferentes tecnologías de gestión (ej. OMA, DM, BBF TR069).
MGR-005	El sistema oneM2M proveerá la capacidad de gestionar múltiples dispositivos de manera agrupada.
MGR-006	El sistema oneM2M proporcionará la capacidad de suministrar y configurar dispositivos de redes M2M.
MGR-007	El sistema oneM2M proveerá la capacidad de monitorización y diagnóstico de dispositivos/gateways en redes M2M.
MGR-008	El sistema oneM2M permitirá la gestión de software de dispositivos en redes M2M.
MGR-009	El sistema oneM2M proveerá la capacidad de reinicio y/o reseteo de

	dispositivos/gateways M2M y otros dispositivos en redes M2M.
MGR-010	El sistema oneM2M proveerá la capacidad de autorizar a dispositivos el acceso a redes M2M.
MGR-011	El sistema oneM2M soportará la capacidad para modificar la topología de dispositivos en redes M2M, sujeta a restricciones basadas en las políticas de las redes M2M.
MGR-012	Tras la detección de un nuevo dispositivo, la infraestructura de servicios M2M deberá provisionar al gateway M2M de una configuración adecuada, necesaria para manejar el dispositivo detectado.
MGR-014	El sistema oneM2M será capaz de recuperar eventos e información registrada por gateways/dispositivos M2M y otros dispositivos en redes M2M.
MGR-015	El sistema oneM2M será capaz de gestionar firmware (ej. actualización) de gateways/dispositivos M2M y otros dispositivos en redes M2M.
MGR-016	El sistema oneM2M será capaz de recuperar información relacionada con el contexto dinámico y estático de dispositivos/gateways M2M así como el contexto de dispositivo para otros dispositivos en redes M2M.
MGR-017	El sistema oneM2M será capaz de relacionar elementos de gestión de acceso, proporcionados por los protocolos de gestión de dispositivo de tecnología específica, y elementos de gestión de acceso usados por el sistema oneM2M.

En la versión borrador de este documento se están discutiendo requisitos adicionales que no serán tenidos en consideración por no estar consensuados a la fecha de este informe.

3.2.3. REQUISITOS DE ABSTRACCIÓN

ID	DESCRIPCIÓN
ABR-001	El sistema oneM2M definirá la estructura de un modelo de Información con el propósito de intercambiar datos.
ABR-002	El sistema oneM2M será capaz de proveer mecanismos de traducción entre Modelos de Información usados por las distintas Aplicaciones y dispositivos/gateways M2M y otros dispositivos.
ABR-003	El sistema oneM2M debe proporcionar capacidades para representar dispositivos y objetos virtuales.

En la versión borrador de este documento [15] se están discutiendo requisitos adicionales que no serán tenidos en consideración por no estar consensuados a la fecha de este informe.

3.2.4. REQUISITOS SEMÁNTICOS

ID	DESCRIPCIÓN
SMR-001	El sistema M2M proveerá capacidades de gestión de descripciones semánticas de recursos y aplicaciones M2M, como por ejemplo crear, obtener, actualizar, borrar o asociar.
SMR-002	El sistema oneM2M soportará un sistema de modelado común de descripciones semánticas (incluyendo relaciones entre objetos) para que puedan ser usadas por Aplicaciones M2M.
SMR-003	El sistema oneM2M proveerá capacidades de cooperación entre diferentes lenguajes de modelado para las descripciones semánticas.
SMR-004	El sistema oneM2M proveerá capacidades de descubrimiento de Recursos M2M basados en descripciones semánticas.
SMR-005	El sistema oneM2M soportará el acceso a descripciones semánticas externas al sistema oneM2M.
SMR-006	El sistema oneM2M será capaz de realizar análisis de datos M2M basados en descripciones semánticas de aplicaciones M2M y/o del sistema oneM2M.
SMR-007	El sistema oneM2M será capaz de realizar Mash-up semánticos usando datos M2M de Aplicaciones M2M y/o del sistema oneM2M (ej. Crear Dispositivos Virtuales, ofrecer nuevos servicios M2M, etc.).

En la versión borrador de este documento [15] se están discutiendo requisitos adicionales que no serán tenidos en consideración por no estar consensuados a la fecha de este informe.

3.2.5. REQUISITOS DE SEGURIDAD

ID	DESCRIPCIÓN
SER-001	El sistema oneM2M incorporará medidas de protección contra amenazas a su disponibilidad tales como ataques DoS (Denial of Service).
SER-002	El sistema oneM2M será capaz de asegurar la confidencialidad de los datos.
SER-003	El sistema oneM2M podrá asegurar la integridad de los datos.

SER-004	En los casos donde los dispositivos M2M soporten USIM/UICC y las redes subyacentes soporten seguridad en la capa de red, el sistema oneM2M podrá aprovechar las credenciales USIM/UICC del dispositivo y las capacidades de seguridad de la red, ej.usar 3GPP GBA para establecer el nivel de seguridad a través de los interfaces a la red subyacente de las aplicaciones y servicios M2M.
SER-005	En los casos donde los dispositivos M2M soporten USIM/UICC y la red soporte seguridad en la capa de red, y cuando el sistema oneM2M conozca la capacidad de arranque de la red subyacente, (ej. 3GPP GBA), el sistema oneM2M será capaz de darla a conocer a servicios y aplicaciones M2M a través de APIs.
SER-006	En los casos donde los dispositivos M2M soportan USIM/UICC y la red soporta seguridad en la capa de red, el sistema oneM2M será capaz de hacer uso de las credenciales USIM/UICC del dispositivo, cuando sea posible, para la asociación de seguridad M2M en los procedimientos de arranque.
SER-007	Cuando algunos de los componentes de una solución M2M no estén disponibles (ej. pérdida de conexión con una WAN), el sistema oneM2M permitirá la confidencialidad e integridad de los datos entre componentes autorizados de la solución M2M que estén disponibles.
SER-008	El sistema oneM2M dispondrá de medidas contra el acceso no autorizado a servicios M2M y a servicios de aplicación M2M.
SER-009	El sistema oneM2M soportará autentificación mutua para las interacciones con redes, servicios M2M y servicios de aplicaciones M2M.
SER-010	El sistema oneM2M tendrá mecanismos para la protección contra el uso indebido, clonado, sustitución o robo de credenciales de seguridad.
SER-011	El sistema oneM2M protegerá el uso de la identidad de un cliente M2M dentro del sistema contra el descubrimiento y el uso indebido por otros clientes.
SER-012	El sistema oneM2M soportará medidas contra ataques de suplantación de identidad y de retransmisión.
SER-013	El sistema oneM2M proveerá mecanismos para comprobar la integridad de componentes software/hardware/firmware en dispositivos M2M al inicio, periódicamente en tiempo de ejecución y en actualizaciones software.
SER-014	El sistema oneM2M proveerá datos de configuración a una aplicación M2M autenticada y autorizada en el dispositivo/gateway M2M.
SER-015	El sistema oneM2M tendrá mecanismos para proveer identidades de suscriptores a aplicaciones M2M autenticadas y autorizadas, siempre

	y cuando el sistema oneM2M tenga el consentimiento del suscriptor.
SER-016	El sistema oneM2M soportará procedimientos de no rechazo dentro de la capa de servicio M2M y en sus interacciones autorizadas con la red y las capas de aplicación.
SER-017	El sistema oneM2M será capaz de mitigar amenazas identificadas en oneM2M ETSI TR 118 508.
SER-018	El sistema oneM2M permitirá a un cliente M2M usar un recurso o servicio y será el responsable de ese uso sin la exposición de su identidad a otros clientes.
SER-019	El sistema oneM2M podrá usar credenciales a nivel de servicio dentro del dispositivo M2M para establecer el nivel de seguridad de aplicaciones y servicios M2M.
SER-020	El sistema oneM2M permitirá a proveedores de servicio M2M legítimos provisionar sus propias credenciales en los dispositivos/gateways M2M.
SER-021	El sistema oneM2M podrá, de forma remota y segura, provisionar credenciales de seguridad M2M en dispositivos/gateways M2M.
SER-022	El sistema oneM2M permitirá a proveedores de servicio de aplicación M2M autorizar interacciones que involucren a sus aplicaciones M2M en entidades permitidas (ej. Dispositivos/Gateways/Infraestructura de servicios).
SER-023	Donde se soporte el uso de módulos de seguridad hardware (Hardware Security Module, HSM), el sistema oneM2M deberá permitir la provisión de seguridad local según el HSM.
SER-024	El sistema oneM2M permitirá a aplicaciones M2M el uso de entornos de seguridad diferentes y separados.
SER-025	El sistema oneM2M evitará que elementos M2M no autorizados identifiquen y/u observen las acciones de otros participantes del sistema oneM2M, ej. su acceso a recursos y servicios.
SER-026	El sistema oneM2M proveerá mecanismos para la protección de la confidencialidad de la información de localización geográfica.

En la versión borrador de este documento se están discutiendo requisitos adicionales que no serán tenidos en consideración por no estar consensuados a la fecha de este informe.

3.2.6. REQUISITOS DE TARIFICACIÓN

ID	DESCRIPCIÓN
CHG-	El sistema oneM2M soportará la recopilación de información específica

001	de tarificación relacionada con los servicios individuales facilitados por el sistema oneM2M (ej. Gestión de datos, de dispositivos y/o de conectividad). La recopilación de dicha información se hará de forma simultánea al uso de los recursos. El formato de la información registrada será totalmente especificado, incluyendo elementos obligatorios y opcionales.
CHG-002	El sistema oneM2M soportará mecanismos para facilitar la correlación de información de tarificación (ej. de un usuario) recopilada por servicios M2M, servicios de aplicación M2M y servicios proporcionados por los operadores de la red.
CHG-003	El sistema oneM2M proporcionará medios para coordinar los registros de datos de tarificación para los usos de datos con diferente calidad de servicio de la red subyacente.
CHG-004	El sistema oneM2M podrá utilizar mecanismos de tarificación existentes en las redes subyacentes.
CHG-005	El sistema oneM2M permitirá la transferencia de los registros de información de tarificación al dominio de facturación del proveedor de servicio M2M, con el propósito de: • Facturación de abonados. • Facturación entre proveedores. • Contabilidad proveedor-abonado, incluyendo funciones adicionales, como estadísticas.
CHG-006	El sistema oneM2M tiene que permitir la generación de eventos de tarificación con el propósito de solicitar permiso para el uso de recursos al sistema de control de crédito en tiempo real, donde la cuenta del abonado esté localizada. La información contenida en los eventos de tarificación y los eventos tarificables relevantes estará totalmente especificada, incluyendo elementos obligatorios y opcionales.

3.2.7. REQUISITOS OPERACIONALES

ID	DESCRIPCIÓN
OPR-001	El sistema oneM2M proporcionará la capacidad de monitorización y diagnóstico de aplicaciones M2M.
OPR-002	El sistema oneM2M proporcionará la capacidad de gestión software de aplicaciones M2M.
OPR-003	El sistema oneM2M será capaz de configurar el estado de ejecución de aplicaciones M2M (iniciarlas, pararlas, reiniciarlas).
OPR-004	Cuando la red subyacente suministre interfaces apropiados, el sistema oneM2M tendrá la habilidad de programar el tráfico a través

	de la red subyacente según instrucciones recibidas de dicha red.
OPR-005	El sistema oneM2M será capaz de intercambiar información con las aplicaciones M2M relacionada con el uso y las características del tráfico de los dispositivos/gateways M2M por parte de la aplicación M2M. Se debe incluir soporte para la característica de 3GPP llamada "Time controlled".
OPR-006	Dependiendo de la disponibilidad de interfaces apropiados proporcionados por la red subyacente, el sistema oneM2M será capaz de proporcionar información a dicha red relacionada con el uso y las características del tráfico de los dispositivos/gateways M2M.

En la versión borrador de este documento [15] se están discutiendo requisitos adicionales que no serán tenidos en consideración por no estar consensuados a la fecha de este informe.

3.2.8. REQUISITOS DE GESTIÓN DE LA COMUNICACIÓN

ID	DESCRIPCIÓN
CRPR-001	El sistema oneM2M proporcionará a aplicaciones M2M un servicio de comunicación que proporcione buffering de los mensajes a/desde gateways, dispositivos o dominio infraestructural M2M.
CRPR-002	El sistema oneM2M será capaz de reenviar los mensajes almacenados en el buffer según las políticas de comunicación y basándose en la preferencia del servicio asociada con los mensajes.
CRPR-003	El sistema oneM2M permitirá que una aplicación M2M envíe una petición de comunicación con la siguiente preferencia de servicio: • Parámetros QoS, incluyendo tolerancia al retardo, para el inicio de la entrega de datos. • Categorización de las peticiones de comunicación en diferentes niveles de prioridad o clases de QoS.
CRPR-004	El sistema oneM2M soportará el procesado concurrente de mensajes dentro de los gateways y/o los dispositivos M2M de diferente origen, teniendo en cuenta la preferencia de servicio asociada a los mensajes junto con las políticas de comunicación proporcionadas.
CRPR-005	El sistema oneM2M deberá mantener el contexto asociado a las sesiones M2M (ej. contexto de seguridad o conectividad de red durante la interrupción de la sesión).

En la versión borrador de este documento [15] se están discutiendo requisitos adicionales que no serán tenidos en consideración por no estar consensuados a la fecha de este informe.

3.2.9. REQUISITOS NO FUNCIONALES (NO NORMATIVOS)

ID	DESCRIPCIÓN
NFR-001	Continua Health Alliance está incorporando una aproximación RESTful a su diseño. Para soportar CHA, oneM2M debe considerar estilos y enfoques RESTful para el diseño de la arquitectura M2M.
NFR-002	El sistema oneM2M debe comunicarse usando protocolos eficientes en términos de cantidad de información intercambiada sobre la cantidad de datos intercambiados, medidos en bytes.

3.3. COMPARATIVA DE REQUISITOS

La siguiente tabla muestra la correspondencia entre los requisitos del UNE 178104 [12] y los del sistema oneM2M [15].

Requisitos UNE 178104	Requisitos oneM2M TS-0002
REP-001: La plataforma debe albergar un catálogo común, universal, mantenido, accesible y clasificado de datos únicos y normalizados de la ciudad (el mantenimiento de los mismo seguirá siendo responsabilidad de los sistemas de gestión que los generan).	OSR-019 El sistema oneM2M debe soportar la capacidad de repositorio de datos (ej. recopilación/almacenamiento) y de transferencia de datos desde uno o más dispositivos/gateways M2M hacia uno o más gateways M2M, infraestructuras de servicios M2M o infraestructuras de aplicaciones M2M, de la forma requerida por la infraestructura de aplicación M2M como se muestra debajo: • Acción iniciada tanto por un dispositivo M2M, un gateway M2M, infraestructuras de servicios M2M o infraestructuras de aplicaciones M2M. • Iniciada por un evento o una activación programada. • Para datos específicos.
	OSR-021 El sistema oneM2M debe proveer mecanismos para permitir la compartición de datos entre múltiples aplicaciones M2M.
	SMR-002 El sistema oneM2M soportará un sistema de modelado común de descripciones semánticas (incluyendo relaciones entre objetos) para que puedan ser usadas por Aplicaciones M2M.
	ABR-001 El sistema oneM2M definirá la estructura de un modelo de Información con el propósito de intercambiar datos.
REP-002 La plataforma debe albergar un catálogo que debe contener también datos sobre los	OSR-019 El sistema oneM2M debe soportar la capacidad de repositorio de datos

activos, ya que la gestión de los mismos es cada vez más relevante en los proyectos de Smart Cities. La normalización de la nomenclatura a utilizar para los activos así como la información requerida dependiendo del tipo que sea cada uno de ellos, es muy importante para que las aplicaciones de gestión de los mismos los reconozcan y se garantice la interoperabilidad.	(ej. recopilación/almacenamiento) y de transferencia de datos desde uno o más dispositivos/gateways M2M hacia uno o más gateways M2M, infraestructuras de servicios M2M o infraestructuras de aplicaciones M2M, de la forma requerida por la infraestructura de aplicación M2M como se muestra debajo: ● Acción iniciada tanto por un dispositivo M2M, un gateway M2M, infraestructuras de servicios M2M o infraestructuras de aplicaciones M2M. ● Iniciada por un evento o una activación programada. ● Para datos específicos.
	OSR-021 El sistema oneM2M debe proveer mecanismos para permitir la compartición de datos entre múltiples aplicaciones M2M.
	SMR-002 El sistema oneM2M soportará un sistema de modelado común de descripciones semánticas (incluyendo relaciones entre objetos) para que puedan ser usadas por Aplicaciones M2M.
	ABR-003 El sistema oneM2M debe proporcionar capacidades para representar dispositivos y objetos virtuales.
REP-003 La plataforma debe permitir visiones analíticas transversales de la ciudad a partir de estos datos.	OSR-036 El sistema oneM2M debe proveer mecanismos para aceptar peticiones de aplicaciones proveedoras de servicios M2M para realizar servicios de analítica.
REP-004 La plataforma debe facilitar y universalizar la integración de datos de alta y baja latencia y del legacy de soluciones existentes en la ciudad.	OSR-002a El sistema oneM2M debe permitir medios de comunicación con dispositivos con capacidades reducidas de computación (ej. CPU, memoria o batería reducidas) o de comunicación (ej. módem inalámbrico 2G).

	OSR-002b El sistema oneM2M debe permitir medios de comunicación con dispositivos con elevadas capacidades de computación (ej. CPU, memoria o batería de complejidad avanzada) o de comunicación (ej. módem inalámbrico 3G).
	OSR-012 El sistema oneM2M debe soportar comunicaciones entre aplicaciones M2M y dispositivos soportando servicios M2M por medio de una conectividad continua o no-continua.
	OSR-015 El sistema oneM2M debe ser capaz de ayudar a las redes subyacentes que soportan diferentes esquemas de comunicación, incluyendo comunicaciones poco frecuentes, transferencia de pequeñas cantidades de datos, transferencia de grandes archivos y comunicaciones en modo streaming.
	OSR-053 El sistema oneM2M debe proveer un medio que permita la compatibilidad hacia atrás de interfaces entre diferentes versiones.
REP-005 La plataforma debe explotar los datos de Ciudad y ofrecer las interfaces para el desarrollo de aplicaciones Smart a partir de ellos, conforme a permisos de acceso a la información adecuados a cada actor específico.	OSR-059 El sistema oneM2M debe ser capaz de permitir control de acceso basado en roles según las suscripciones a servicios M2M.
INFR-001 Debe soportar acceso a los datos de plataformas de sensores, bases de datos y a información de otras aplicaciones.	OSR-049 El sistema oneM2M debe proveer la capacidad para que una aplicación M2M pueda compartir datos entre Aplicaciones de forma selectiva.
	OSR-054 El sistema oneM2M debe permitir que una aplicación, un dispositivo, o un gateway M2M obtengan acceso a los recursos de otra aplicación, dispositivo o gateway M2M.
	OSR-055 El sistema oneM2M debe proveer la capacidad de que las aplicaciones

	M2M intercambien datos con una o más aplicaciones M2M que no sean conocidas de antemano.
INFR-002 La plataforma debe permitir actuaciones sobre actuadores (sensores) a través de soluciones estandarizadas.	OSR-008 El sistema oneM2M debe proveer la capacidad para que aplicaciones M2M se comunique con dispositivos M2M (ej. una aplicación en un dispositivo), sin la necesidad de conocer la tecnología o el protocolo de comunicación específico de dichos dispositivos M2M.
	OPR-003 El sistema oneM2M será capaz de configurar el estado de ejecución de aplicaciones M2M (iniciarlas, pararlas, reiniciarlas).
	MGR-014 El sistema oneM2M será capaz de recuperar eventos e información registrada por gateways/dispositivos M2M y otros dispositivos en redes M2M.
INFR-004 La plataforma debe soportar la gestión del mantenimiento de equipos e infraestructuras.	OPR-001 El sistema oneM2M proporcionará la capacidad de monitorización y diagnóstico de aplicaciones M2M.
	MGR-001 El sistema oneM2M podrá soportar la gestión y la configuración de dispositivos/gateways M2M incluyendo dispositivos M2M con recursos limitados.
	MGR-004 El sistema oneM2M soportará mecanismos comunes de gestión de dispositivos mediante diferentes tecnologías de gestión (ej. OMA, DM, BBF TR069).
	MGR-006 El sistema oneM2M proporcionará la capacidad de suministrar y configurar dispositivos de redes M2M.
INFR-005 La plataforma debe soportar protocolos estándar de monitorización como SNMP y JMX.	MGR-007 El sistema oneM2M proveerá la capacidad de monitorización y diagnóstico de dispositivos/gateways en redes M2M.

INFR-006 La plataforma debe permitir la integración con otros sistemas y aplicaciones.	OSR-007 El sistema oneM2M debe proveer un mecanismo para que las aplicaciones M2M interactúen con las aplicaciones y con los datos/información gestionados por un proveedor de servicio M2M diferente, sujeto a los permisos apropiados.
	OSR-021 El sistema oneM2M debe proveer mecanismos para permitir la compartición de datos entre múltiples aplicaciones M2M.
INT-001 La plataforma debe proveer las interfaces necesarias para que eventos de un sistema puedan desencadenar acciones en otros.	OSR-028 El sistema oneM2M debe permitir a una aplicación M2M definir condiciones de activación en el sistema, tales que éste pueda enviar de forma autónoma comandos a actuadores en nombre de la aplicación M2M cuando las mencionadas condiciones se cumplan.
INT-002 La plataforma debe usar APIs y protocolos normalizados para la comunicación entre aplicaciones.	OSR-003 El sistema oneM2M debe soportar comunicaciones entre aplicaciones (A2A) en coordinación con una sesión de aplicación para las aplicaciones M2M que lo requieran.
	OSR-021 El sistema oneM2M debe proveer mecanismos para permitir la compartición de datos entre múltiples aplicaciones M2M.
	OSR-054 El sistema oneM2M debe permitir que una aplicación, un dispositivo, o un gateway M2M obtengan acceso a los recursos de otra aplicación, dispositivo o gateway M2M.
	OSR-055 El sistema oneM2M debe proveer la capacidad de que las aplicaciones M2M intercambien datos con una o más aplicaciones M2M que no sean conocidas de antemano.
INT-003 La plataforma debe tener la capacidad de extenderse para soportar otros protocolos de comunicación con sensores.	OSR-041 El sistema oneM2M debe proveer un mecanismo que soporte la inclusión de nuevos servicios M2M en un sistema oneM2M, implementados

	como módulos transferibles independientes por medio de las interfaces de oneM2M.
SEC-001 La plataforma debe soportar autenticación y autorización.	SER-008 El sistema oneM2M dispondrá de medidas contra el acceso no autorizado a servicios M2M y a servicios de aplicación M2M.
	SER-009 El sistema oneM2M soportará autentificación mutua para las interacciones con redes, servicios M2M y servicios de aplicaciones M2M.
SEC-002 La plataforma debe controlar el acceso a la plataforma y a todos los elementos a los que se acceda a través de esta: sensores, scadas, centros de control, bases de datos y aplicaciones a las que se acceda a través de ella.	SER-008 El sistema oneM2M dispondrá de medidas contra el acceso no autorizado a servicios M2M y a servicios de aplicación M2M.
SEC-003 La plataforma debe garantizar confidencialidad en la comunicación con la Plataforma.	SER-011 El sistema oneM2M protegerá el uso de la identidad de un cliente M2M dentro del sistema contra el descubrimiento y el uso indebido por otros clientes.
	SER-025 El sistema oneM2M evitará que elementos M2M no autorizados identifiquen y/u observen las acciones de otros participantes del sistema oneM2M, ej. su acceso a recursos y servicios.
SEC-004 La plataforma debe garantizar confidencialidad en el acceso a los datos, de modo que cada rol sólo pueda ver los datos a los que tiene acceso.	SER-002 El sistema oneM2M será capaz de asegurar la confidencialidad de los datos.
	SER-003 El sistema oneM2M podrá asegurar la integridad de los datos.
	SER-008 El sistema oneM2M dispondrá de medidas contra el acceso no autorizado a servicios M2M y a servicios de aplicación M2M.

SEC-005 La plataforma debe definir y gestionar políticas de seguridad	OSR-059 El sistema oneM2M debe ser capaz de permitir control de acceso basado en roles según las suscripciones a servicios M2M.
SEC-006 La plataforma debe proveer un módulo central y de fácil acceso (vía web) para poder realizar gestiones de administración de los usuarios, roles y permisos	*Aunque la gestión de permisos, usuarios y roles de considera en el TS-0001 no se especifica que la gestión tenga que realizarse a través de web.*
SEC-007 La plataforma debe soportar diferentes mecanismos de autenticación como soluciones basadas en usuario y contraseña en tokens, en OAuth, en certificados electrónicos (de individuos, servidores y aplicaciones) u otro tipo de soluciones avanzadas basadas, por ejemplo, en técnicas biométricas.	SER-008 El sistema oneM2M dispondrá de medidas contra el acceso no autorizado a servicios M2M y a servicios de aplicación M2M.
	SER-009 El sistema oneM2M soportará autentificación mutua para las interacciones con redes, servicios M2M y servicios de aplicaciones M2M.
	SER-019 El sistema oneM2M podrá usar credenciales a nivel de servicio dentro del dispositivo M2M para establecer el nivel de seguridad de aplicaciones y servicios M2M.
	SER-020 El sistema oneM2M permitirá a proveedores de servicio M2M legítimos provisionar sus propios credenciales en los dispositivos/gateways M2M.
	SER-021 El sistema oneM2M podrá, de forma remota y segura, provisionar credenciales de seguridad M2M en dispositivos/gateways M2M.
SEC-008 La plataforma debe permitir la integración con repositorio de usuarios ya existentes en la AAPP, del estilo LDAP, Base de Datos de usuarios,etc.	*El sistema oneM2M no implementa la integración con repositorios de usuarios, aunque una aplicación oneM2M que sirviera de puente entre ambas podría ser implementada.*
SEC-009 La plataforma debe tener capacidad de extender para adaptar los mecanismos de seguridad a las necesidades propias de cada ciudad	*El sistema oneM2M soporta varios mecanismos de seguridad que podrían ser usados según interese para la aplicación a desarrollar.*

SEC-010 La plataforma debe asegurar la privacidad y seguridad de los datos almacenados o gestionados por la solución, especialmente en un entorno compartido de recursos (PaaS: Plataforma como Servicio). Asimismo, se deben poder definir distintos perfiles de acceso a los diferentes tipos/grupos de datos, que eviten un uso inadecuado de los mismos.	OSR-059 El sistema oneM2M debe ser capaz de permitir control de acceso basado en roles según las suscripciones a servicios M2M.
	SER-002 El sistema oneM2M será capaz de asegurar la confidencialidad de los datos.
SEC-011 La plataforma debe garantizar el envío y recepción segura de datos desde y hacia los dispositivos conectados a ella, así como su distribución segura a los aplicativos que los requieran. Como mínimo debe implementar la autenticación de los elementos que originan los datos y de los aplicativos que requieren acceso a dichos datos.	OSR-010 El sistema oneM2M debe soportar mecanismos de confirmación de la correcta entrega de mensajes a su destino, a aquellas aplicaciones M2M que requieran un envío confiable para detectar fallos en mensajes en un intervalo de tiempo dado.
	OSR-011a El sistema oneM2M debe ser capaz de solicitar diferentes caminos de comunicación de la red subyacente, basándose en las reglas del proveedor de servicios M2M o del operador de red, con mecanismos de enrutamiento para evitar fallos en la transmisión.
	SER-007 Cuando algunos de los componentes de una solución M2M no estén disponibles (ej. pérdida de conexión con una WAN), el sistema oneM2M permitirá la confidencialidad e integridad de los datos entre componentes autorizados de la solución M2M que estén disponibles.
SEC-012 La plataforma debe permitir definir diferentes roles y niveles de acceso sobre los datos, funcionalidades y servicios de la plataforma, autorizar o denegar el acceso a los distintos aplicativos y definir los privilegios requeridos para actuar sobre un determinado conjunto de datos. Los usuarios de la Plataforma Integrada pueden ser individuos o aplicaciones que consuman servicios o información. Hay que considerar diferentes tipos de acceso: usuario de la plataforma (persona a través de consola o web, aplicaciones a través de los servicios y APIs), usuarios internos, terceros, de confianza, etc, con diferentes roles:	OSR-023 El sistema oneM2M debe ser capaz de identificar los servicios M2M a usar por parte de las diferentes suscripciones de Servicio M2M.
	OSR-024 El sistema oneM2M debe ser capaz de identificar los dispositivos M2M a usar por parte de las diferentes suscripciones de Servicio M2M.
	OSR-025 El sistema oneM2M debe ser capaz de identificar las aplicaciones M2M a usar por parte de las diferentes suscripciones de Servicio M2M.

Administrador del sistema. Operador Directivos Clientes sw de otras aplicaciones etc. La gestión de roles/permisos se establecerá como mínimo respecto a tres niveles de seguridad: **a. Acceso a los datos:** limitar la información que puede visualizar cada usuario. Por ejemplo: a un usuario de un determinado Servicio sólo tendrá acceso a la información correspondiente a los datos de su Servicio, datos generales como medidas globales, desviaciones y otros que se obtengan del tratamiento conjunto de los datos correspondientes a todos los Servicios. **Acceso a los elementos de la Plataforma Integral:** limitar el acceso a los informes y cuadro de mando configurados en la Plataforma Integral Por ejemplo un usuario de un Servicio sólo podrá acceder a los informes definidos con los datos correspondiente a su ámbito **Funcionalidad:** delimitar las acciones que puede realizar un determinado usuario en función de su perfil	OSR-059 El sistema oneM2M debe ser capaz de permitir control de acceso basado en roles según las suscripciones a servicios M2M. SER-022 El sistema oneM2M permitirá a proveedores de servicio de aplicación M2M autorizar interacciones que involucren a sus aplicaciones M2M en entidades permitidas (ej. Dispositivos, Gateways, infraestructura de servicios).
MANT-001 La plataforma debe facilitar el almacenamiento y valoración de indicadores relevantes para la gestión del mantenimiento.	*La versión actual del documento de requisitos publicado por oneM2M no recoge como tal el concepto de indicadores, aunque si las capacidades de monitorización y gestión de dispositivos y aplicaciones.*
MANT-002 La plataforma debe facilitar la generación de planes de mantenimiento a partir de indicadores relevantes para la gestión del mantenimiento.	*La versión actual del documento de requisitos publicado por oneM2M no recoge como tal el concepto de indicadores, aunque si las capacidades de monitorización y gestión de dispositivos y aplicaciones.*
MANT-003 La plataforma debe permitir la posibilidad de gestionar los avisos o alarmas y poder enviar mensajes, correos, SMS, llamadas en función de indicadores relevantes para la gestión del mantenimiento.	OSR-005 El sistema oneM2M debe ser capaz de descubrirlos servicios ofrecidos por redes de comunicación a aplicaciones M2M (ej. SMS, USSD, localización, configuración de suscripción, autenticación, etc) sujetos a las reglas de restricciones del correspondiente operador de red. OSR-006 El sistema oneM2M debe ser capaz

	de reutilizar servicios ofrecidos por las redes subyacentes a aplicaciones/servicios M2M,a través de modelos de acceso abierto(ej. OMA, framework GSMA OneAPI). Algunos ejemplos de servicios disponibles son: • Comunicaciones IP multimedia. • Mensajería • Localización. • Servicios de tarificación y facturación. • Información de dispositivos y perfiles. • Configuración y gestión de dispositivos. • Activación [JM2] y monitorización de dispositivos. • Pequeñas transmisiones de datos. • Gestión de grupos.
	OSR-040 El sistema oneM2M debe poder hacer uso de múltiples mecanismos de comunicación (tales como USSD o SMS) cuando estén disponibles en las redes subyacentes.
MANT-004 La plataforma debe permitir la posibilidad de integración nativa con sistemas móviles y apps.	*La versión actual del documento de requisitos publicado por oneM2M no recoge como tal ningún requisito equivalente.*
APP-001 La plataforma debe permitir realizar análisis de consumos, alarmas, tendencias, etc.	*La versión actual del documento de requisitos publicado por oneM2M no recoge como tal ningún requisito que considere todos estos aspectos.*
APP-002 La plataforma debe permitir realizar imputación de costes.	CHG-001 El sistema oneM2M soportará la recopilación de información específica de tarificación relacionada con los servicios individuales facilitados por el sistema oneM2M (ej. Gestión de datos, de dispositivos y/o de conectividad). La recopilación de dicha información se hará de forma simultánea al uso de los recursos. El formato de la información registrada será totalmente especificado, incluyendo elementos obligatorios y opcionales.
	CHG-002 El sistema oneM2M soportará

	mecanismos para facilitar la correlación de información de tarificación (ej. de un usuario) recopilada por servicios M2M, servicios de aplicación M2M y servicios proporcionados por los operadores de la red.
	CHG-003 El sistema oneM2M proporcionará medios para coordinar los registros de datos de tarificación para los usos de datos con diferente calidad de servicio de la red subyacente.
	CHG-004 El sistema oneM2M podrá utilizar mecanismos de tarificación existentes en las redes subyacentes.
	CHG-005 El sistema oneM2M permitirá la transferencia de los registros de información de tarificación al dominio de facturación del proveedor de servicio M2M, con el propósito de: • Facturación de abonados. • Facturación entre proveedores. • Contabilidad proveedor-abonado, incluyendo funciones adicionales, como estadísticas.
	CHG-006 El sistema oneM2M tiene que permitir la generación de eventos de tarificación con el propósito de solicitar permiso para el uso de recursos al sistema de control de crédito en tiempo real, donde la cuenta del abonado esté localizada. La información contenida en los eventos de tarificación y los eventos tarificables relevantes estará totalmente especificada, incluyendo elementos obligatorios y opcionales.
APP-003 La plataforma debe permitir la sostenibilidad (uso eficiente de las instalaciones, emisiones, etc.)	OSR-035 El sistema oneM2M debe permitir el intercambio de información relevante de aplicaciones no-M2M (ej. Clases de dispositivos/gateways) entre

	dispositivos/gateways M2M e infraestructuras de servicios M2M con el propósito de facilitar una comunicación eficiente. Esto incluye la capacidad de que un dispositivo M2M informe de su clase de dispositivo a la infraestructura de servicio M2M y de que la infraestructura de servicio M2M informe de sus capacidades al dispositivo M2M.
APP-004 La plataforma debe permitir realizar optimización de procesos y planificación.	*La versión actual del documento de requisitos publicado por oneM2M no recoge como tal ningún requisito equivalente.*
APP-005 La plataforma debe permitir realizar un control de calidad de servicios públicos por terceros.	*La versión actual del documento de requisitos publicado por oneM2M no recoge como tal ningún requisito equivalente.*
APP-006 La plataforma debe permitir realizar una sala de crisis.	*La versión actual del documento de requisitos publicado por oneM2M no recoge como tal ningún requisito equivalente.*
APP-007 La plataforma debe soportar la generación de informes de explotación.	*La versión actual del documento de requisitos publicado por oneM2M no recoge como tal ningún requisito equivalente.*
APP-008 La plataforma debe poder integrarse con herramientas para el análisis de todos estos indicadores.	*La versión actual del documento de requisitos publicado por oneM2M no recoge como tal el concepto de indicadores, aunque si las capacidades de monitorización y gestión de dispositivos y aplicaciones.*
DSS-001 La plataforma debe integrar herramientas de simulación en base a la información actual e histórica.	*La versión actual del documento de requisitos publicado por oneM2M no recoge como tal ningún requisito equivalente ya que se trata de algo específico para la Plataforma de Gestión de Ciudades.*
DSS-002 La plataforma debe integrar herramientas de valoración y ejecución de planes de actuación, en escenarios complejos.	*La versión actual del documento de requisitos publicado por oneM2M no recoge como tal ningún requisito equivalente ya que se trata de algo específico para la Plataforma de Gestión de Ciudades.*

DSS-003 La plataforma debe integrar herramientas de análisis predictivo y modelado de la ciudad.	*La versión actual del documento de requisitos publicado por oneM2M no recoge como tal ningún requisito equivalente ya que se trata de algo específico para la Plataforma de Gestión de Ciudades.*
DSS-004 La plataforma debe integrar herramientas de minería de datos y el análisis estadístico.	*La versión actual del documento de requisitos publicado por oneM2M no recoge como tal ningún requisito equivalente ya que se trata de algo específico para la Plataforma de Gestión de Ciudades.*
DSS-005 La plataforma debe integrar herramientas de integración con otros sistemas y herramientas del BI.	*La versión actual del documento de requisitos publicado por oneM2M no recoge como tal ningún requisito equivalente ya que se trata de algo específico para la Plataforma de Gestión de Ciudades.*
PUBL-001 La plataforma debe permitir transmitir información abierta y en formatos estándar.	ABR-002 El sistema oneM2M será capaz de proveer mecanismos de traducción entre Modelos de Información usados por las distintas Aplicaciones y dispositivos/gateways M2M y otros dispositivos.
	SMR-002 El sistema oneM2M soportará un sistema de modelado común de descripciones semánticas (incluyendo relaciones entre objetos) para que puedan ser usadas por Aplicaciones M2M.
PUBL-002 La plataforma debe permitir transmitir información fidedigna y de calidad.	SER-003 El sistema oneM2M podrá asegurar la integridad de los datos.
PUBL-003 La plataforma debe permitir transmitir información accesible a multidispositivos.	ABR-002 El sistema oneM2M será capaz de proveer mecanismos de traducción entre Modelos de Información usados por las distintas Aplicaciones y dispositivos/gateways M2M y otros dispositivos.
PUBL-004 La plataforma debe permitir transmitir información de forma continua y sin interrupciones.	OSR-022 Cuando algunos de los componentes de una solución oneM2M no estén disponibles (ej. Conexión WAN pérdida), el sistema oneM2M deberá permitir el correcto funcionamiento del resto de componentes

	disponibles de dicha solución oneM2M.
	OSR-034 El sistema oneM2M debe permitir el reemplazo sin interrupción de dispositivos M2M así como de gateways M2M (ej. redirección de tráfico, conexión, recuperación, etc.).
PUBL-005 La plataforma debe permitir transmitir información aplicable a servicios finalistas al ciudadano (sociedad de la información).	*La versión actual del documento de requisitos publicado por oneM2M no recoge como tal ningún requisito equivalente ya que se trata de algo específico para la Plataforma de Gestión de Ciudades.*
PUBL-006 La plataforma debe permitir transmitir información aplicable a aplicaciones de terceros (open data).	ABR-002 El sistema oneM2M será capaz de proveer mecanismos de traducción entre Modelos de Información usados por las distintas Aplicaciones y dispositivos/gateways M2M y otros dispositivos.
PUBL-007 La plataforma debe permitir transmitir información aplicable a otros servicios públicos y administraciones.	*La versión actual del documento de requisitos publicado por oneM2M no recoge como tal ningún requisito equivalente ya que se trata de algo específico para la Plataforma de Gestión de Ciudades.*
PUBL-008 La plataforma debe permitir transmitir información aplicable a rendición de cuentas (transparencia).	*La versión actual del documento de requisitos publicado por oneM2M no recoge como tal ningún requisito equivalente ya que se trata de algo específico para la Plataforma de Gestión de Ciudades.*
FALL-001 La plataforma debe garantizar la continuidad operativa de los servicios inteligentes de acuerdo con los niveles de servicios contratados. Estos servicios podrían requerir disponibilidad 24x7 y un nivel de servicio superior al 99.9% anual y se incluirán en las métricas. El proveedor deberá ofrecer soluciones que garanticen funcionamiento ante cualquier incidente o emergencia, necesarias para cumplir este requisito.	OSR-022 Cuando algunos de los componentes de una solución oneM2M no estén disponibles (ej. Conexión WAN pérdida), el sistema oneM2M deberá permitir el correcto funcionamiento del resto de componentes disponibles de dicha solución oneM2M.
	OSR-034 El sistema oneM2M debe permitir el reemplazo sin interrupción de dispositivos M2M así como de gateways M2M (ej. redirección de tráfico, conexión, recuperación, etc.).

FALL-002 La plataforma debe garantizar la recuperación en caso de desastres como un RTO (Objetivo de Tiempo de Recuperación) y un RPO (Objetivo de Punto de Recuperación) limitados, que se valorarán en las métricas.	OSR-022 Cuando algunos de los componentes de una solución oneM2M no estén disponibles (ej. Conexión WAN pérdida), el sistema oneM2M deberá permitir el correcto funcionamiento del resto de componentes disponibles de dicha solución oneM2M.
RTEC-001 Horizontalidad: capacidad de soporte de diferentes ámbitos de aplicación, de manera que sea posible la implementación simultánea de múltiples servicios en la misma infraestructura.	OSR-009 El sistema oneM2M debe soportar la capacidad de que una o múltiples aplicaciones M2M interactúen con uno o múltiples dispositivos/gateways M2M (aplicación en el dispositivo/gateway).
RTEC-002 Interoperabilidad: capacidad de soporte de diferentes tecnologías, dispositivos y mecanismos de captura de información, y estándares de comunicación, así como otros sistemas de información internos/corporativos y/o externos.	OSR-008 El sistema oneM2M debe proveer la capacidad para que aplicaciones M2M se comunique con dispositivos M2M (ej. una aplicación en un dispositivo), sin la necesidad de conocer la tecnología o el protocolo de comunicación específico de dichos dispositivos M2M.
	OSR-021 El sistema oneM2M debe proveer mecanismos para permitir la compartición de datos entre múltiples aplicaciones M2M.
	OSR-055 El sistema oneM2M debe proveer la capacidad de que las aplicaciones M2M intercambien datos con una o más aplicaciones M2M que no sean conocidas de antemano.
	SMR-005 El sistema oneM2M soportará el acceso a descripciones semánticas externas al sistema oneM2M.
RTEC-003 Rendimiento: habilidad del sistema para manejar en tiempo real un elevado número de dispositivos, servicios y procesos de manera eficiente.	OSR-029 El sistema oneM2M debe poder enviar comandos comunes a varios actuadores o sensores a través de un grupo.
RTEC-004 Escalabilidad: capacidad de poder incrementar capacidad de proceso y almacenamiento sin tener que modificar la arquitectura.	*La versión actual del documento de requisitos publicado por oneM2M no recoge como tal ningún requisito equivalente.*

RTEC-005 Robustez y Resiliencia: capacidad para seguir funcionando ante problemas.	OSR-022 Cuando algunos de los componentes de una solución oneM2M no estén disponibles (ej. Conexión WAN pérdida), el sistema oneM2M deberá permitir el correcto funcionamiento del resto de componentes disponibles de dicha solución oneM2M.
	OSR-034 El sistema oneM2M debe permitir el reemplazo sin interrupción de dispositivos M2M así como de gateways M2M (ej. redirección de tráfico, conexión, recuperación, etc.).
RTEC-006 Modularidad: la plataforma debe tener un enfoque modular que permite desplegarla por partes (por ejemplo, módulo Big Data) de forma sencilla.	OSR-041 El sistema oneM2M debe proveer un mecanismo que soporte la inclusión de nuevos servicios M2M en un sistema oneM2M, implementados como módulos transferibles independientes por medio de las interfaces de oneM2M.
RTEC-007 Continuidad operativa o disponibilidad: capacidad del sistema para estar operativo en cualquier momento.	OSR-034 El sistema oneM2M debe permitir el reemplazo sin interrupción de dispositivos M2M así como de gateways M2M (ej. redirección de tráfico, conexión, recuperación, etc.).
RTEC-008 Capacidad de Recuperación: capacidad para gestionar de forma eficiente los fallos que puedan afectar a la disponibilidad.	OSR-022 Cuando algunos de los componentes de una solución oneM2M no estén disponibles (ej. Conexión WAN pérdida), el sistema oneM2M deberá permitir el correcto funcionamiento del resto de componentes disponibles de dicha solución oneM2M.
	OSR-034 El sistema oneM2M debe permitir el reemplazo sin interrupción de dispositivos M2M así como de gateways M2M (ej. redirección de tráfico, conexión, recuperación, etc.).
RTEC-009 Flexibilidad: habilidad de la plataforma para funcionar con diferentes servicio inteligentes de ciudad.	OSR-041 El sistema oneM2M debe proveer un mecanismo que soporte la inclusión de nuevos servicios M2M en un sistema oneM2M, implementados

	como módulos transferibles independientes por medio de las interfaces de oneM2M.
RTEC-010 Extensibilidad: capacidad de la plataforma para poder ampliarse para dar soporte a nuevas necesidades.	OSR-041 El sistema oneM2M debe proveer un mecanismo que soporte la inclusión de nuevos servicios M2M en un sistema oneM2M, implementados como módulos transferibles independientes por medio de las interfaces de oneM2M.
RTEC-011 Capacidades Big Data: para integrar una gran cantidad de datos generados desde múltiples fuentes y con diferentes estructuras.	*Hace falta un módulo Big Data desplegado en forma de aplicación oneM2M para el tratamiento Big Data de los datos obtenidos de los sensores.*
RTEC-012 Basada en estándares abiertos: lo que simplifica la integración con otras plataformas y el desarrollo de aplicaciones sobre la Plataforma que puedan ser reusables y portables entre diferentes plataformas.	*oneM2M en sí mismo es un estándar abierto.*
RTEC-013 Evolucionable: facilitando su capacidad de extensión en el futuro mediante estándares ampliamente adoptados.	OSR-041 El sistema oneM2M debe proveer un mecanismo que soporte la inclusión de nuevos servicios M2M en un sistema oneM2M, implementados como módulos transferibles independientes por medio de las interfaces de oneM2M.
RTEC-014 Integral: la plataforma debe trabajar como un todo, no como piezas desacopladas que no están preparadas para trabajar en conjunto.	*La versión actual del documento de requisitos publicado por oneM2M no recoge como tal ningún requisito equivalente.*
RTEC-015 Operable y gestionable: la plataforma debe poder gestionar, operar, mantener e instalarse de forma sencilla.	*La versión actual del documento de requisitos publicado por oneM2M no recoge como tal ningún requisito equivalente.*
RTEC-016 Semántica: el uso de conceptos semánticos en la Plataforma permite la interoperabilidad entre plataformas y por tanto entre ciudades.	ABR-002 El sistema oneM2M será capaz de proveer mecanismos de traducción entre Modelos de Información usados por las distintas Aplicaciones y dispositivos/gateways M2M y otros dispositivos.
	SMR-002 El sistema oneM2M soportará un sistema de modelado común de descripciones semánticas

	(incluyendo relaciones entre objetos) para que puedan ser usadas por Aplicaciones M2M.
	SMR-003 El sistema oneM2M proveerá capacidades de cooperación entre diferentes lenguajes de modelado para las descripciones semánticas.
	SMR-005 El sistema oneM2M soportará el acceso a descripciones semánticas externas al sistema oneM2M.
RTEC-017 Seguridad: garantía del sistema en cuanto a seguridad, privacidad y confianza se refiere.	*Recogido en varios requisitos de seguridad del oneM2M.*
ARQ-001 La plataforma se ajusta al sistema de capas propuesto en el documento.	*No aplica en el oneM2M.*
ADQ-001 Independencia del operador de red.	OSR-005 El sistema oneM2M debe ser capaz de descubrirlos servicios ofrecidos por redes de comunicación a aplicaciones M2M (ej. SMS, USSD, localización, configuración de suscripción, autenticación, etc.) sujetos a las reglas de restricciones del correspondiente operador de red.
	OSR-006 El sistema oneM2M debe ser capaz de reutilizar servicios ofrecidos por las redes subyacentes a aplicaciones/servicios M2M,a través de modelos de acceso abierto(ej. OMA, framework GSMA OneAPI). Algunos ejemplos de servicios disponibles son: • Comunicaciones IP multimedia. • Mensajería • Localización. • Servicios de tarificación y facturación. • Información de dispositivos y perfiles. • Configuración y gestión de dispositivos. • Activación [JM2] y monitorización de dispositivos. • Pequeñas transmisiones de datos.

	• Gestión de grupos.
	OSR-011b El sistema oneM2M debe ser capaz de solicitar diferentes caminos de comunicación de la red subyacente según las peticiones de las aplicaciones M2M.
	OSR-017 El sistema oneM2M debe ser capaz de ofrecer acceso a diferentes tipos de servicios M2M a los proveedores de servicios M2M. Estos servicios han de incluir, como mínimo: • Gestión de la conectividad. • Gestión de dispositivos (a nivel de servicio). • Gestión de datos de aplicación. Para permitir distintos escenarios de desarrollo, estos servicios han de ser ofrecidos por el sistema oneM2M, individualmente, como un subconjunto o un conjunto completo de servicios.
	OSR-018 El sistema oneM2M debe ser capaz de ofrecer servicios M2M a dispositivos M2M en itinerancia a través las redes celulares subyacentes, según restricciones basadas en las reglas del operador de red.
	OSR-027 El sistema M2M debe proveer un mecanismo genérico para permitir el intercambio transparente de datos entre la aplicación M2M y la red subyacente, sujeto a las restricciones basadas en la política del proveedor de servicios M2M y/o en la del operador de red.
	OSR-040 El sistema oneM2M debe poder hacer uso de múltiples mecanismos de comunicación (tales como USSD o SMS) cuando estén disponibles en las redes subyacentes.
	OSR-050 Si la comunicación mediante un canal proporcionado por la red subyacente solo puede ser activada unidireccionalmente (Dominio de

	campo o dominio de infraestructura), y hay canales alternativos disponibles en la otra dirección, el sistema oneM2M debe poder usar estos canales alternativos para activar la comunicación bidireccional en el primer canal.
ADQ-002 Integración de la información desde las fuentes de datos (sensores, dispositivos etc…).	OSR-001 El sistema oneM2M debe permitir comunicación entre aplicaciones M2M usando múltiples medios de comunicación basados en acceso mediante IP.
	OSR-002a El sistema oneM2M debe permitir medios de comunicación con dispositivos con capacidades reducidas de computación (ej. CPU, memoria o batería reducidas) o de comunicación (ej. módem inalámbrico 2G).
	OSR-002b El sistema oneM2M debe permitir medios de comunicación con dispositivos con elevadas capacidades de computación (ej. CPU, memoria o batería de complejidad avanzada) o de comunicación (ej. módem inalámbrico 3G).
	OSR-014 El sistema oneM2M debe ser capaz de comunicarse con dispositivos M2M, conectados a través de un Gateway M2M capaz de soportar redes M2M heterogéneas.
	OSR-016 El sistema oneM2M debe proveer la capacidad de notificar a aplicaciones M2M de la disponibilidad, o cambios, de aplicaciones o información de gestión de un dispositivo/gateway M2M disponible, incluyendo cambios en la red M2M.
	OSR-044 El sistema oneM2M debe soportar comunicación tanto con dispositivos M2M que son accesibles de forma programada (ej. periódica), como también con dispositivos M2M que son accesibles de una forma

	espontánea e impredecible.
	OSR-045a El sistema oneM2M debe poder recibir y utilizar información obtenida de la red subyacente sobre cuándo un dispositivo M2M puede ser accedido.
	MGR-002 El sistema oneM2M será capaz de descubrir redes M2M, incluyendo información sobre sus dispositivos y los parámetros de dichas redes (ej. topología, protocolo).
	MGR-003 El sistema oneM2M será capaz de proveer la capacidad de mantener y describir el modelo de información de gestión de los dispositivos y parámetros (ej. topología, protocolo) de redes M2M.
	MGR-006 El sistema oneM2M proporcionará la capacidad de suministrar y configurar dispositivos de redes M2M.
ADQ-003 Suministrar la información a la capa de conocimiento con independencia de los dispositivos dando una vista semántica de los datos adquiridos.	ABR-001 El sistema oneM2M definirá la estructura de un modelo de Información con el propósito de intercambiar datos.
	ABR-002 El sistema oneM2M será capaz de proveer mecanismos de traducción entre Modelos de Información usados por las distintas Aplicaciones y dispositivos/gateways M2M y otros dispositivos.
	ABR-003 El sistema oneM2M debe proporcionar capacidades para representar dispositivos y objetos virtuales.
	SMR-001 El sistema M2M proveerá capacidades de gestión de descripciones semánticas de recursos y aplicaciones M2M, como por ejemplo crear, obtener, actualizar, borrar o asociar.

	SMR-002 El sistema oneM2M soportará un sistema de modelado común de descripciones semánticas (incluyendo relaciones entre objetos) para que puedan ser usadas por Aplicaciones M2M.
	SMR-003 El sistema oneM2M proveerá capacidades de cooperación entre diferentes lenguajes de modelado para las descripciones semánticas.
ADQ-004 Se adapta el modelo ETSI M2M. Tiene interfaces abiertos y estandarizados sobre los que será posible desarrollar aplicaciones de terceros que interactúen directamente con los dispositivos, no propietarios.	*oneM2M se adapta completamente al modelo ETSI M2M.*
ADQ-005 Solución de capa de adquisición única para distintos servicios.	OSR-009 El sistema oneM2M debe soportar la capacidad de que una o múltiples aplicaciones M2M interactúen con uno o múltiples dispositivos/gateways M2M (aplicación en el dispositivo/gateway).
ADQ-006 Independencia de la tecnología de acceso y sensores.	OSR-008 El sistema oneM2M debe proveer la capacidad para que aplicaciones M2M se comunique con dispositivos M2M (ej. una aplicación en un dispositivo), sin la necesidad de conocer la tecnología o el protocolo de comunicación específico de dichos dispositivos M2M.
ADQ-007 Posibilidad de añadir nuevos conectores.	OSR-041 El sistema oneM2M debe proveer un mecanismo que soporte la inclusión de nuevos servicios M2M en un sistema oneM2M, implementados como módulos transferibles independientes por medio de las interfaces de oneM2M.
ADQ-008 Acceso a los sensores	OSR-008 El sistema oneM2M debe proveer la capacidad para que aplicaciones M2M se comunique con dispositivos M2M (ej. una aplicación en un dispositivo), sin la necesidad de conocer la tecnología o el protocolo

	de comunicación específico de dichos dispositivos M2M.
	OSR-002a El sistema oneM2M debe permitir medios de comunicación con dispositivos con capacidades reducidas de computación (ej. CPU, memoria o batería reducidas) o de comunicación (ej. módem inalámbrico 2G).
	OSR-002b El sistema oneM2M debe permitir medios de comunicación con dispositivos con elevadas capacidades de computación (ej. CPU, memoria o batería de complejidad avanzada) o de comunicación (ej. módem inalámbrico 3G).
ADQ-009 Módulo capaz de conectar escenarios compatibles con oneM2M.	*Compatibilidad entre los dos estándares*
CON-001 Acceso a toda la información tanto histórica como en tiempo real	OSR-016 El sistema oneM2M debe proveer la capacidad de notificar a aplicaciones M2M de la disponibilidad, o cambios, de aplicaciones o información de gestión de un dispositivo/gateway M2M disponible, incluyendo cambios en la red M2M.
	OSR-019 El sistema oneM2M debe soportar la capacidad de repositorio de datos (ej. recopilación/almacenamiento) y de transferencia de datos desde uno o más dispositivos/gateways M2M hacia uno o más gateways M2M, infraestructuras de servicios M2M o infraestructuras de aplicaciones M2M, de la forma requerida por la infraestructura de aplicación M2M como se muestra debajo: • Acción iniciada tanto por un dispositivo M2M, un gateway M2M, infraestructuras de servicios M2M o infraestructuras de aplicaciones M2M. • Iniciada por un evento o una activación programada. • Para datos específicos.

	OSR-020 El sistema oneM2M debe admitir reglas sobre los aspectos de almacenamiento y recuperación de datos/información, así como gestión de las mismas.
	OSR-033 El sistema oneM2M debe proveer la capacidad de ajustar dinámicamente la programación de informes y notificaciones de un dispositivo/gateway M2M, basándose en el contexto de dispositivos/gateways dinámicos del dispositivo/gateway M2M y en las categorías de eventos previamente definidas.
	MGR-014 El sistema oneM2M será capaz de recuperar eventos e información registrada por gateways/dispositivos M2M y otros dispositivos en redes M2M.
CON-002 Movimiento de datos recibidos por la capa de adquisición para almacenamiento, proceso y recuperación y a disposición de la capa de interoperabilidad siguiendo modelos de datos	ABR-001 El sistema oneM2M definirá la estructura de un modelo de Información con el propósito de intercambiar datos.
	ABR-002 El sistema oneM2M será capaz de proveer mecanismos de traducción entre Modelos de Información usados por las distintas Aplicaciones y dispositivos/gateways M2M y otros dispositivos.
	SMR-002 El sistema oneM2M soportará un sistema de modelado común de descripciones semánticas (incluyendo relaciones entre objetos) para que puedan ser usadas por Aplicaciones M2M.
CON-003 Soporte tratamiento en tiempo real de los datos recibidos de la capa de adquisición a través de motor de reglas, etc…	OSR-019 El sistema oneM2M debe soportar la capacidad de repositorio de datos (ej. recopilación/almacenamiento) y de transferencia de datos desde uno o más dispositivos/gateways M2M hacia uno o más gateways M2M, infraestructuras de servicios M2M o infraestructuras de aplicaciones

	M2M, de la forma requerida por la infraestructura de aplicación M2M como se muestra debajo: • Acción iniciada tanto por un dispositivo M2M, un gateway M2M, infraestructuras de servicios M2M o infraestructuras de aplicaciones M2M. • Iniciada por un evento o una activación programada. • Para datos específicos.
	OSR-028 El sistema oneM2M debe permitir a una aplicación M2M definir condiciones de activación en el sistema, tales que éste pueda enviar de forma autónoma comandos a actuadores en nombre de la aplicación M2M cuando las mencionadas condiciones se cumplan.
CON-004 Soporte en tratamiento Batch de los datos recibidos a través de ETL ("Extraer, transformar y cargar").	*La versión actual del documento de requisitos publicado por oneM2M no recoge como tal ningún requisito equivalente ya que se trata de algo específico para la Plataforma de Gestión de Ciudades.*
CON-005 Soporte Tratamiento analítico de los datos mediante proceso BI (Business Intelligence).	*La versión actual del documento de requisitos publicado por oneM2M no recoge como tal ningún requisito equivalente ya que se trata de algo específico para la Plataforma de Gestión de Ciudades.*
CON-006 Soporte tratamiento GIS, permitiendo georeferencias de datos y hacer consultas geográficas.	OSR-037 El sistema oneM2M debe permitir a cualquier aplicación M2M solicitar el envío de datos, de forma independiente de la red subyacente, a las aplicaciones M2M de un grupo de dispositivos y gateways M2M, en zonas geográficas especificadas por la aplicación M2M.
	OSR-047 El sistema oneM2M debe soportar mecanismos para que los dispositivos M2M y/o Gateways informen sobre su localización geográfica a aplicaciones M2M.
	OSR-048

	El sistema oneM2M debe proveer un servicio M2M que permita a dispositivos M2M y/o Gateways compartir su información de localización geográfica o la de otros dispositivos M2M.
	OSR-051 Dependiendo de la disponibilidad de interfaces apropiados proporcionados por la red subyacente, el sistema oneM2M debe poder pedir a la red que retransmita datos en modo broadcast/multicast a un grupo de dispositivos M2M en un área específica.
CON-007 Seguridad: se controla usuario/rol para cada dato.	OSR-059 El sistema oneM2M debe ser capaz de permitir control de acceso basado en roles según las suscripciones a servicios M2M.
CON-008 Aplicar semántica creadas por organización internacionales como por ejemplo el vocabulario e-Goverment Core desarrollado por el programa ISA o las listas de códigos, glosarios y tesauros de Eurostats.	*No se define ninguna semántica específica en oneM2M.*
CINT-001 Publicación de APIs que garanticen la portabilidad de aplicaciones entre ciudades y plataformas, debe ser de tipo REST con diferentes modos de acceso (Incluyendo modo Push y Pull) así como consultas georeferenciadas.	OSR-008 El sistema oneM2M debe proveer la capacidad para que aplicaciones M2M se comunique con dispositivos M2M (ej. una aplicación en un dispositivo), sin la necesidad de conocer la tecnología o el protocolo de comunicación específico de dichos dispositivos M2M.
CINT-002 Capacidad de interconexión con aplicaciones y plataformas.	OSR-003 El sistema oneM2M debe soportar comunicaciones entre aplicaciones (A2A) en coordinación con una sesión de aplicación para las aplicaciones M2M que lo requieran.
	OSR-007 El sistema oneM2M debe proveer un mecanismo para que las aplicaciones M2M interactúen con las aplicaciones y con los datos/información gestionados por un proveedor de servicio M2M diferente, sujeto a los permisos apropiados.

	OSR-021 El sistema oneM2M debe proveer mecanismos para permitir la compartición de datos entre múltiples aplicaciones M2M.
	OSR-054 El sistema oneM2M debe permitir que una aplicación, un dispositivo, o un gateway M2M obtengan acceso a los recursos de otra aplicación, dispositivo o gateway M2M.
	OSR-055 El sistema oneM2M debe proveer la capacidad de que las aplicaciones M2M intercambien datos con una o más aplicaciones M2M que no sean conocidas de antemano.
CINT-003 Acceso a servicios externos.	OSR-007 El sistema oneM2M debe proveer un mecanismo para que las aplicaciones M2M interactúen con las aplicaciones y con los datos/información gestionados por un proveedor de servicio M2M diferente, sujeto a los permisos apropiados.
CINT-004 Publicación de un portal opendata.	*No se recoge en el oneM2M.*
CINT-005 Kit de desarrollo con SDK y APIs para construir servicios (Aplicaciones de movilidad, de calidad del aire, de eficiencia energética, riego inteligente…) de un forma sencilla por la comunidad de desarrolladores.	*Los servicios en oneM2M se pueden desarrollar usando los protocolos CoaP, MQTT y RESTfull para interactuar con el sistema.*
CINT-006 Modelo de acceso a datos agnóstico. Se recomienda el modelo oneM2M.	*Compatibilidad entre ambos estándares.*
SER-001 Centro de mandos personalizados e indicadores para diferentes ubicaciones de despliegue en función del perfil y de los permisos del usuario.	OSR-023 El sistema oneM2M debe ser capaz de identificar los servicios M2M a usar por parte de las diferentes suscripciones de Servicio M2M.
	OSR-024 El sistema oneM2M debe ser capaz de identificar los dispositivos M2M a usar por parte de las diferentes suscripciones de Servicio M2M.
	OSR-025 El sistema oneM2M debe ser capaz de identificar las aplicaciones M2M a

	usar por parte de las diferentes suscripciones de Servicio M2M.
SER-002 Aplicaciones de gestión de los servicios verticales desarrollados anteriormente para la ciudad como pueden ser sistemas de calidad de agua, eficiencia energética en edificios públicos, parking inteligente…	*No se especifica como requisito pero si se aplica como casos de uso dentro de oneM2M.*
SER-003 Aplicaciones de gestión de los contratos (SLA en bases de datos).	CRPR-003 El sistema oneM2M permitirá que una aplicación M2M envíe una petición de comunicación con la siguiente preferencia de servicio: • Parámetros QoS, incluyendo tolerancia al retardo, para iniciar la entrega de datos. • Categorización de las peticiones de comunicación en diferentes niveles de prioridad o clases de QoS.
	OSR-038 El sistema oneM2M debe soportar la inclusión de preferencias de calidad de servicio (QoS) de aplicaciones M2M en peticiones de servicio a la red subyacente.
	OSR-039 El sistema oneM2M debe poder autorizar peticiones de servicio con preferencias QoS a nivel de servicio, pero las preferencias de QoS de aplicaciones M2M deben ser pasadas a las redes subyacentes en las solicitudes de servicio, para llevar a cabo la autorización y concesión o negociación de las peticiones de QoS de servicio.
	OSR-042 El sistema oneM2M debe soportar diferentes niveles de QoS, identificando parámetros tales como la tasa de bit garantizada, retardo, variaciones de retardo, tasa de pérdidas y tasa de error, etc.
SOP-001 Entorno Web de Gestión de la configuración permitiendo a través de una aplicación Web de gestión de toda esta, incluyendo interfaces REST de gestión.	*La versión actual del documento de requisitos publicado por oneM2M no recoge como tal ningún requisito equivalente.*

SOP-002 Repositorio de configuración de la plataforma de modo que existe un lugar centralizado de almacenamiento de toda esta.	MGR-016 El sistema oneM2M será capaz de recuperar información relacionada con el contexto dinámico y estático de dispositivos/gateways M2M así como el contexto de dispositivo para otros dispositivos en redes M2M.
SOP-003 Seguridad de acceso (Usuario y que rol tiene para acceder a los datos) y Conectores de Repositorio de Seguridad de modo que la seguridad pueda delegarse al gestor de usuarios de la ciudad.	OSR-059 El sistema oneM2M debe ser capaz de permitir control de acceso basado en roles según las suscripciones a servicios M2M.
IPL-001 Independencia en el dominio de las apps.	OSR-007 El sistema oneM2M debe proveer un mecanismo para que las aplicaciones M2M interactúen con las aplicaciones y con los datos/información gestionados por un proveedor de servicio M2M diferente, sujeto a los permisos apropiados.
	OSR-055 El sistema oneM2M debe proveer la capacidad de que las aplicaciones M2M intercambien datos con una o más aplicaciones M2M que no sean conocidas de antemano.
IPL-002 Independencia en el dominio de la red.	OSR-006 El sistema oneM2M debe ser capaz de reutilizar servicios ofrecidos por las redes subyacentes a aplicaciones/servicios M2M, a través de modelos de acceso abierto(ej. OMA, framework GSMA OneAPI). Algunos ejemplos de servicios disponibles son: • Comunicaciones IP multimedia. • Mensajería • Localización. • Servicios de tarificación y facturación. • Información de dispositivos y perfiles. • Configuración y gestión de dispositivos. • Activación [JM2] y monitorización de dispositivos. • Pequeñas transmisiones de datos. • Gestión de grupos.

IPL-003 Independencia en el dominio del sistema de adquisición.	OSR-008 El sistema oneM2M debe proveer la capacidad para que aplicaciones M2M se comunique con dispositivos M2M (ej. una aplicación en un dispositivo), sin la necesidad de conocer la tecnología o el protocolo de comunicación específico de dichos dispositivos M2M.
MET-001 Grado de adecuación al modelo de capas y funcionalidades.	*No aplica en el oneM2M.*
MET-002 Modularidad de la Plataforma.	OSR-041 El sistema oneM2M debe proveer un mecanismo que soporte la inclusión de nuevos servicios M2M en un sistema oneM2M, implementados como módulos transferibles independientes por medio de las interfaces de oneM2M.
MET-003 Integración con otras Plataformas.	OSR-008 El sistema oneM2M debe proveer la capacidad para que aplicaciones M2M se comunique con dispositivos M2M (ej. una aplicación en un dispositivo), sin la necesidad de conocer la tecnología o el protocolo de comunicación específico de dichos dispositivos M2M.
	OSR-021 El sistema oneM2M debe proveer mecanismos para permitir la compartición de datos entre múltiples aplicaciones M2M.
	OSR-055 El sistema oneM2M debe proveer la capacidad de que las aplicaciones M2M intercambien datos con una o más aplicaciones M2M que no sean conocidas de antemano.
	SMR-005 El sistema oneM2M soportará el acceso a descripciones semánticas externas al sistema oneM2M.
	OSR-003 El sistema oneM2M debe soportar comunicaciones entre aplicaciones (A2A) en coordinación con una sesión de aplicación para las aplicaciones M2M que lo requieran.

	OSR-021 El sistema oneM2M debe proveer mecanismos para permitir la compartición de datos entre múltiples aplicaciones M2M.
	OSR-054 El sistema oneM2M debe permitir que una aplicación, un dispositivo, o un gateway M2M obtengan acceso a los recursos de otra aplicación, dispositivo o gateway M2M.
	OSR-055 El sistema oneM2M debe proveer la capacidad de que las aplicaciones M2M intercambien datos con una o más aplicaciones M2M que no sean conocidas de antemano.
MET-004 Basarse en estándares abiertos.	*oneM2M se adapta completamente al modelo ETSI M2M.*
	ABR-002 El sistema oneM2M será capaz de proveer mecanismos de traducción entre Modelos de Información usados por las distintas Aplicaciones y dispositivos/gateways M2M y otros dispositivos.
	SMR-002 El sistema oneM2M soportará un sistema de modelado común de descripciones semánticas (incluyendo relaciones entre objetos) para que puedan ser usadas por Aplicaciones M2M.
	oneM2M en sí mismo es un estándar abierto.
MET-005 Protocolos IoT soportados.	*En oneM2M se soportan actualmente para la gestión de dispositivos los protocolos OMA DM y BFF y el acceso a los recursos se puede hacer usando CoAP MQTT y un interfaz RESTFull.*
MET-006 Capacidad de extensión de la Plataforma.	OSR-041 El sistema oneM2M debe proveer un mecanismo que soporte la inclusión de nuevos servicios M2M en un sistema oneM2M, implementados como módulos transferibles independientes por medio de las interfaces de oneM2M.

MET-007 Soporte Enfoque Big Data	*Hace falta un módulo Big Data desplegado en forma de aplicación oneM2M para el tratamiento Big Data de los datos obtenidos de los sensores aunque no se recoge un requisito específico*
MET-008 Soporte Enfoque Opendata	ABR-002 El sistema oneM2M será capaz de proveer mecanismos de traducción entre Modelos de Información usados por las distintas Aplicaciones y dispositivos/gateways M2M y otros dispositivos.
MET-009 Servicio en On premise/cloud.	*La versión actual del documento de requisitos publicado por oneM2M no recoge como tal ningún requisito equivalente.*
MET-010 Inclusión capacidades GIS.	OSR-037 El sistema oneM2M debe permitir a cualquier aplicación M2M solicitar el envío de datos, de forma independiente de la red subyacente, a las aplicaciones M2M de un grupo de dispositivos y gateways M2M,en zonas geográficas especificadas por la aplicación M2M.
	OSR-047 El sistema oneM2M debe soportar mecanismos para que los dispositivos M2M y/o Gateways informen sobre su localización geográfica a aplicaciones M2M.
	OSR-048 El sistema oneM2M debe proveer un servicio M2M que permita a dispositivos M2M y/o Gateways compartir su información de localización geográfica o la de otros dispositivos M2M.
	OSR-051 Dependiendo de la disponibilidad de interfaces apropiados proporcionados por la red subyacente, el sistema oneM2M debe poder pedir a la red que retransmita datos en modo broadcast/multicast a un grupo de dispositivos M2M en un área específica.
MET-011 Inclusión de herramientas de uso y	*La versión actual del documento de requisitos publicado por oneM2M no*

configuración.	*recoge como tal ningún requisito equivalente*
MET-012 Niveles de disponibilidad y nivel de servicio.	OSR-022 Cuando algunos de los componentes de una solución oneM2M no estén disponibles (ej. Conexión WAN pérdida), el sistema oneM2M deberá permitir el correcto funcionamiento del resto de componentes disponibles de dicha solución oneM2M.
	OSR-034 El sistema oneM2M debe permitir el reemplazo sin interrupción de dispositivos M2M así como de gateways M2M (ej. redirección de tráfico, conexión, recuperación, etc.).
MET-013 Garantía, soporte y hoja de ruta.	*No aplica al oneM2M.*

A continuación se recoge una tabla con los requisitos oneM2M que no han podido ser asociados a equivalentes en la norma de Plataforma de Gestión de Ciudad Inteligente.

REQUISITO	COMENTARIOS
OSR-004 El sistema oneM2M debe soportar comunicaciones entre aplicaciones sin establecimiento de sesión para las aplicaciones M2M que lo requieran.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
OSR-013 El sistema oneM2M debe conocer la tolerancia de retardo aceptable por la aplicación M2M y debe programar la comunicación o pedir a la red subyacente que lo haga, según del criterio de reglas definido.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
OSR-026 El sistema oneM2M debe poder asociar los dispositivos M2M usados por las suscripciones de Servicio M2M con los identificadores de dispositivo ofrecidos por la red subyacente y el dispositivo, siempre que la red subyacente lo permita.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
OSR-030 El sistema oneM2M permitir la gestión (ej. Añadir, borrar, modificar y obtener) de los miembros de un grupo.	*En el documento publicado UNE 178 104 no se aborda la gestión de grupos.*
OSR-031 El sistema oneM2M debe permitir a un grupo ser un miembro de otro grupo.	*En el documento publicado UNE 178 104 no se aborda la gestión de grupos.*

OSR-032 El sistema oneM2M debe permitir distintas categorías de evento (ej. normal, urgente) asociadas a la recepción, almacenado o reporte de datos por parte de una aplicación M2M.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
OSR-043 El sistema oneM2M debe poder verificar que miembros de un grupo soportan un conjunto de funciones comunes.	*En el documento publicado UNE 178 104 no se aborda la gestión de grupos.*
OSR-045b El sistema oneM2M debe poder utilizar programaciones de accesibilidad generados tanto por el dispositivo M2M como por el Dominio de la Infraestructura.	*En el documento publicado UNE 178 104 no se abordan horarios ni programación de accesibilidad.*
OSR-046 El sistema oneM2M debe soportar la capacidad de que una aplicación M2M pueda requerir o rechazar confirmación para sus comunicaciones.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
OSR-052 El sistema oneM2M debe poder seleccionar una red apropiada para la difusión/multidifusión (broadcast/multicast) de datos, dependiendo de la capacidades de la red y la conectividad soportada por el grupo seleccionado de dispositivos/gateways M2M.	*En el documento publicado UNE 178 104 no se abordan sus capacidades broadcast/multicast.*
OSR-056 El sistema oneM2M debe permitir el descubrimiento de aplicaciones M2M utilizables, en un gateway o dispositivo M2M.	*En el documento publicado UNE 178 104 no se aborda el descubrimiento de dispositivos.*
OSR-057 El sistema oneM2M debe permitir el descubrimiento de gateways y dispositivos M2M disponibles a una aplicación M2M para el intercambio de datos.	*En el documento publicado UNE 178 104 no se aborda el descubrimiento de dispositivos.*
OSR-058 El sistema oneM2M debe proveer marcas de tiempo según sea necesario para las funciones de servicios comunes.	*En el documento publicado UNE 178 104 no se abordan marcas de tiempo.*
OSR-060 El sistema oneM2M debe permitir la sincronización temporal con un reloj externo.	*En el documento publicado UNE 178 104 no se aborda sincronización temporal.*
OSR-061 Los dispositivos y gateways M2M pueden soportar sincronización temporal conforme al sistema oneM2M.	*En el documento publicado UNE 178 104 no se aborda sincronización temporal.*
OSR-062 El sistema oneM2M debe permitir medios para la comprobaciónde la conectividad entre un conjunto de aplicaciones M2M.	*En el documento publicado UNE 178 104 no se abordan los medios de comprobación de la conectividad.*
OSR-063 El sistema oneM2M debe poder gestionar la	*En el documento publicado UNE 178 104 no se aborda la*

planificación de la conectividad y mensajería de la capa de servicio M2M entre el dominio de infraestructura y los dispositivos/gateways M2M.	*planificación de los mensajes.*
OSR-064 El sistema oneM2M debe poder agrupar mensajes dependiendo de la tolerancia al retardo del mensaje y/o su categoría.	*En el documento publicado UNE 178 104 no se abordan estos aspectos.*
OSR-065 El sistema oneM2M debe proporcionar mecanismos que permitan a un proveedor de servicios M2M distribuir funciones de procesado a sus dispositivos/gateways M2M en el dominio de campo.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
OSR-066 El sistema oneM2M debe permitir la colocación y operación de aplicaciones M2M en nodos M2M seleccionados según criterios requeridos por los proveedores de servicios de aplicación, sujeto a los derechos de acceso.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
OSR-068 Cuando esté disponible en la red subyacente, el sistema oneM2M proveerá la capacidad de obtener y presentar información acerca de si un dispositivo M2M está autorizado a acceder a los servicios de la red subyacente.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
OSR-069 Cuando esté disponible en una red, el sistema oneM2M mantendrá el estado operacional del servicio M2M de un dispositivo M2M y lo actualizará cuando el estado del servicio de conectividad de la red subyacente cambie.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
OSR-070 El sistema oneM2M debe proveer la capacidad de notificar a una aplicación M2M autorizada sobre cuándo el estado administrativo u operacional del servicio M2M de un dispositivo M2M cambie, siempre que esa aplicación M2M esté suscrita a tales notificaciones.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
OSR-071 El sistema oneM2M debe permitir a una aplicación M2M autorizada cambiar el estado administrativo de un servicio M2M en un dispositivo M2M.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
OSR-072 El sistema oneM2M debe poder iniciar un conjunto de acciones bien definidas (ej. activación si sobrepasa un umbral, comparar un valor, etc.) en una o más aplicaciones M2M en nombre de otra aplicación M2M.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
MGR-005 El sistema oneM2M proveerá la capacidad de gestionar múltiples dispositivos de manera agrupada.	*En el documento publicado UNE 178 104 no se aborda la gestión de grupos.*

MGR-008 El sistema oneM2M permitirá la gestión de software de dispositivos en redes M2M.	*En el documento publicado UNE 178 104 no se aborda la gestión de software de los dispositivos.*
MGR-009 El sistema oneM2M proveerá la capacidad de reinicio y/o reseteo de dispositivos/gateways M2M y otros dispositivos en redes M2M.	*En el documento publicado UNE 178 104 no se aborda la capacidad de reiniciar dispositivos/gateways.*
MGR-011 El sistema oneM2M soportará la capacidad para modificar la topología de dispositivos en redes M2M, sujeta a restricciones basadas en las políticas de las redes M2M.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
MGR-012 Tras la detección de un nuevo dispositivo, la infraestructura de servicios M2M deberá provisionar al gateway M2M de una configuración adecuada , necesaria para manejar el dispositivo detectado.	*En el documento publicado UNE 178 104 no se aborda la configuración de nuevos dispositivos.*
MGR-015 El sistema oneM2M será capaz de gestionar firmware (ej. actualización) de gateways/dispositivos M2M y otros dispositivos en redes M2M.	*En el documento publicado UNE 178 104 no se aborda la gestión de firmware.*
MGR-017 El sistema oneM2M será capaz de relacionar elementos de gestión de acceso, proporcionados por los protocolos de gestión de dispositivo de tecnología específica, y elementos de gestión de acceso usados por el sistema oneM2M.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
SMR-004 El sistema oneM2M proveerá capacidades para de descubrimiento de Recursos M2M basados en descripciones semánticas.	*En el documento publicado UNE 178 104 no se aborda el descubrimiento de dispositivos.*
SMR-006 El sistema oneM2M será capaz de realizar análisis de datos M2M basados en descripciones semánticas de aplicaciones M2M y/o del sistema oneM2M.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
SMR-007 El sistema oneM2M será capaz de realizar Mash-up semánticos usando datos M2M de Aplicaciones M2M y/o del sistema oneM2M (ej. Crear Dispositivos Virtuales, ofrecer nuevos servicios M2M, etc.).	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
OPR-002 El sistema oneM2M proporcionará la capacidad de gestión software de aplicaciones M2M.	*En el documento publicado UNE 178 104 no se aborda la gestión software.*
OPR-004 Cuando la red subyacente suministre interfaces apropiados, el sistema oneM2M tendrá la habilidad de programar el tráfico a través de la red subyacente	*En el documento publicado UNE 178 104 no se aborda este aspecto.*

según instrucciones recibidas de dicha red.	
OPR-005 El sistema oneM2M será capaz de intercambiar información con las aplicaciones M2M relacionada con el uso y las características del tráfico de los dispositivos/gateways M2M por parte de la aplicación M2M. Se debe incluir soporte para la característica de 3GPP llamada "Time controlled".	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
OPR-006 Dependiendo de la disponibilidad de interfaces apropiados proporcionados por la red subyacente, el sistema oneM2M será capaz de proporcionar información a dicha red relacionada con el uso y las características del tráfico de los dispositivos/gateways M2M.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
CRPR-001 El sistema oneM2M proporcionará a aplicaciones M2M un servicio de comunicación que proporcione buffering de los mensajes a/desde gateways, dispositivos o dominio infraestructural M2M.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
CRPR -002 El sistema oneM2M será capaz de reenviar los mensajes en el buffer según las políticas de comunicación y basándose en la preferencia de servicio asociada con los mensajes.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
CRPR -004 El sistema oneM2M soportará el procesado concurrente de mensajes dentro de los gateways y/o los dispositivos M2M de diferente origen y teniendo en cuenta la preferencia de servicio asociada a los mensajes y además teniendo en cuenta las políticas de comunicación proporcionadas.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
SER-001 El sistema oneM2M incorporará medidas de protección contra amenazas a su disponibilidad tales como ataques DoS (Denial of Service).	*No se han tenido en cuenta estas amenazas de seguridad en la Plataforma Integral.*
SER-004 En los casos donde los dispositivos M2M soporten USIM/UICC y las redes subyacentes soporten seguridad en la capa de red, el sistema oneM2M podrá aprovechar las credenciales USIM/UICC del dispositivo y las capacidades de seguridad de la red, ej. usar 3GPP GBA para establecer el nivel de seguridad a través de los interfaces a la red subyacente de las aplicaciones y servicios M2M.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
SER-005 En los casos donde los dispositivos M2M soporten USIM/UICC y la red soporte seguridad en la capa de red, y cuando el sistema oneM2M conozca la capacidad de arranque de la red subyacente, (ej.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*

3GPP GBA), el sistema oneM2M será capaz de darla a conocer a servicios y aplicaciones M2M a través de APIs.	
SER-006 En los casos donde los dispositivos M2M soportan USIM/UICC y la red soporta seguridad en la capa de red, el sistema oneM2M será capaz de hacer uso de las credenciales USIM/UICC del dispositivo, cuando sea posible, para la asociación de seguridad M2M en los procedimientos de arranque.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
SER-010 El sistema oneM2M tendrá mecanismos para la protección contra el uso indebido, clonado, sustitución o robo de credenciales de seguridad.	*No se han tenido en cuenta estas amenazas de seguridad en la UNE 178 104.*
SER-012 El sistema oneM2M soportará medidas contra ataques de suplantación de identidad y de retransmisión.	*No se han tenido en cuenta estas amenazas de seguridad en la UNE 178 104.*
SER-013 El sistema oneM2M proveerá mecanismos para comprobar la integridad de componentes software/hardware/firmware en dispositivos M2M al inicio, periódicamente en tiempo de ejecución y en actualizaciones software.	*No se han tenido en cuenta estas amenazas de seguridad en la Plataforma Integral.*
SER-014 El sistema oneM2M proveerá datos de configuración a una aplicación M2M autenticada y autorizada en el dispositivo/gateway M2M.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
SER-015 El sistema oneM2M tendrá mecanismos para proveer identidades de suscriptores a aplicaciones M2M autenticadas y autorizadas, siempre y cuando el sistema oneM2M tenga el consentimiento del suscriptor.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
SER-016 El sistema oneM2M soportará procedimientos de no rechazo dentro de la capa de servicio M2M y en sus interacciones autorizadas con la red y las capas de aplicación.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
SER-017 El sistema oneM2M será capaz de mitigar amenazas identificadas en oneM2M ETSI TR 118 508	*No se han tenido en cuenta estas amenazas de seguridad en la Plataforma Integral.*
SER-023 Donde se soporte el uso de módulos de seguridad hardware (Hardware Security Module, HSM), el sistema oneM2M deberá permitir la provisión de seguridad local según el HSM.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*
SER-024	*En el documento publicado*

El sistema oneM2M permitirá a aplicaciones M2M el uso de entornos de seguridad diferentes y separados.	*UNE 178 104 no se aborda este aspecto.*
SER-026 El sistema oneM2M proveerá mecanismos para la protección de la confidencialidad de la información de localización geográfica.	*En el documento publicado UNE 178 104 no se aborda este aspecto.*

3.3.1. CONCLUSIONES

En resumen y como conclusiones de la comparativa realizada:

- En los documentos analizados de la norma oneM2M se describe a muy bajo nivel la estructura de los recursos del sistema (tanto AEs, CSEs, Contenedores de datos, etc.), su direccionamiento y las primitivas para actuar sobre ellos (CRUD) junto con los distintos efectos sobre dichos recursos. También se incluye una completa descripción de la arquitectura funcional del sistema y sus puntos de referencia o interfaces, así como el detalle de cada una de las funcionalidades definidas.
- Por su parte, la norma UNE 178 104 [12] se centra en la definición de funcionalidades de más alto nivel orientadas a la implementación de sistemas para aplicaciones de ciudad inteligente, junto con la descripción de su arquitectura de capas. En ningún caso se definen de manera explícita ni la estructura interna de los datos, ni la forma de acceso a ellos.
- No se han encontrado requisitos que sean incompatibles entre las dos especificaciones si no que son complementarias entre si y en muchas cuestiones coincidentes. La UNE contempla requisitos específicos aplicables a Sistemas de Gestión de Ciudades Inteligentes mientras que la TS-0001 [14] es más genérica al contemplar también todos los dispositivos y aplicaciones que forman parte de un sistema M2M.

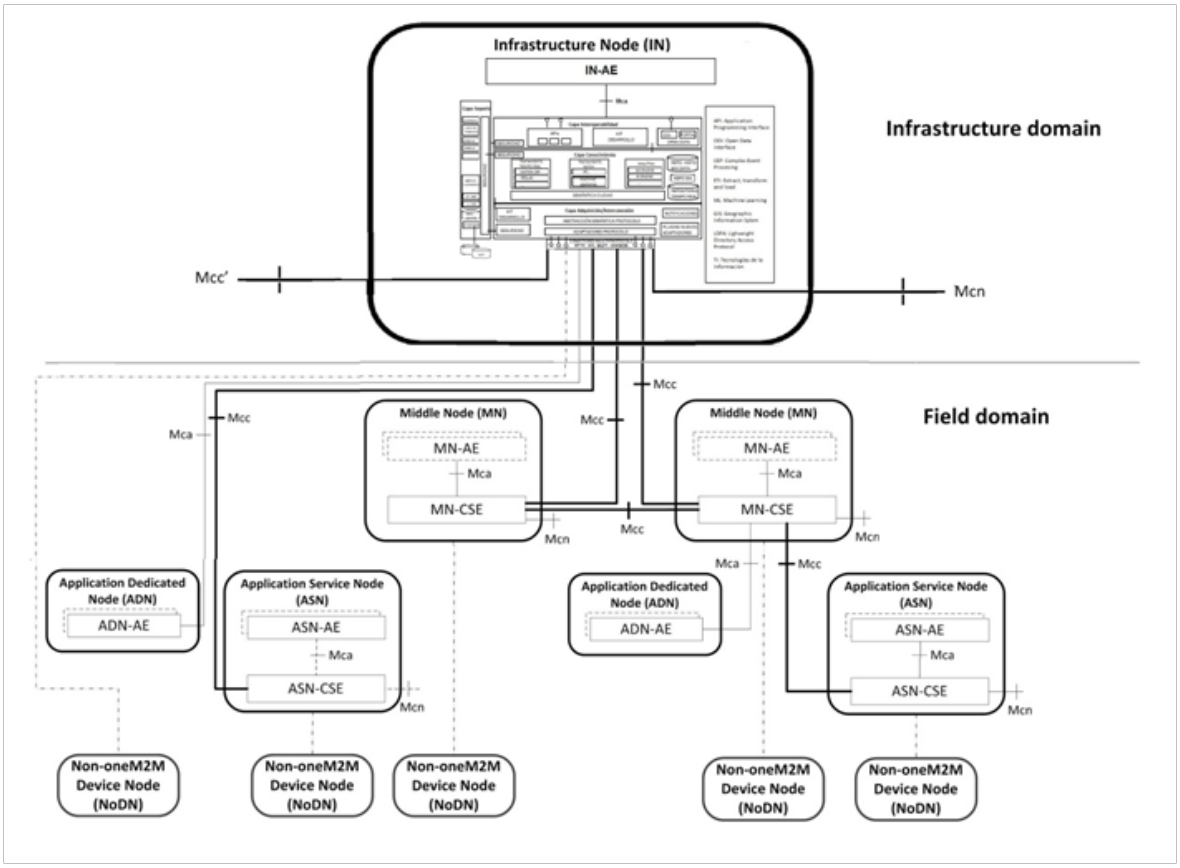
Finalmente, los resultados del análisis realizado pueden organizarse en diversos aspectos:

1. *Estructura funcional:*

Una de las principales diferencias entre los documentos estudiados reside en que la descripción de la Plataforma Integral de Gestión de la Ciudad Inteligente, definida en el documento UNE [12], solo puede hacerse corresponder al Nodo de Infraestructura (IN), definido en la norma oneM2M, mientras que el contenido de la norma oneM2M es aplicable a los distintos gateways, dispositivos y aplicaciones que componen todo el sistema M2M, tal y como se puede comprobar en la figura siguiente, donde se refleja la relación, a nivel de funcionalidad, entre ambos sistemas. En la definición de la estructura funcional que hace oneM2M se distingue entre dominio de campo (“Field Domain”) y dominio de infraestructura (“Infraestructure Domain”). En este contexto, la estructura de capas definida en el documento UNE puede identificarse como parte de los IN que describe oneM2M dentro del dominio de infraestructura, quedando fuera los elementos pertenecientes al sistema de captación y a la red de servicios inteligentes.

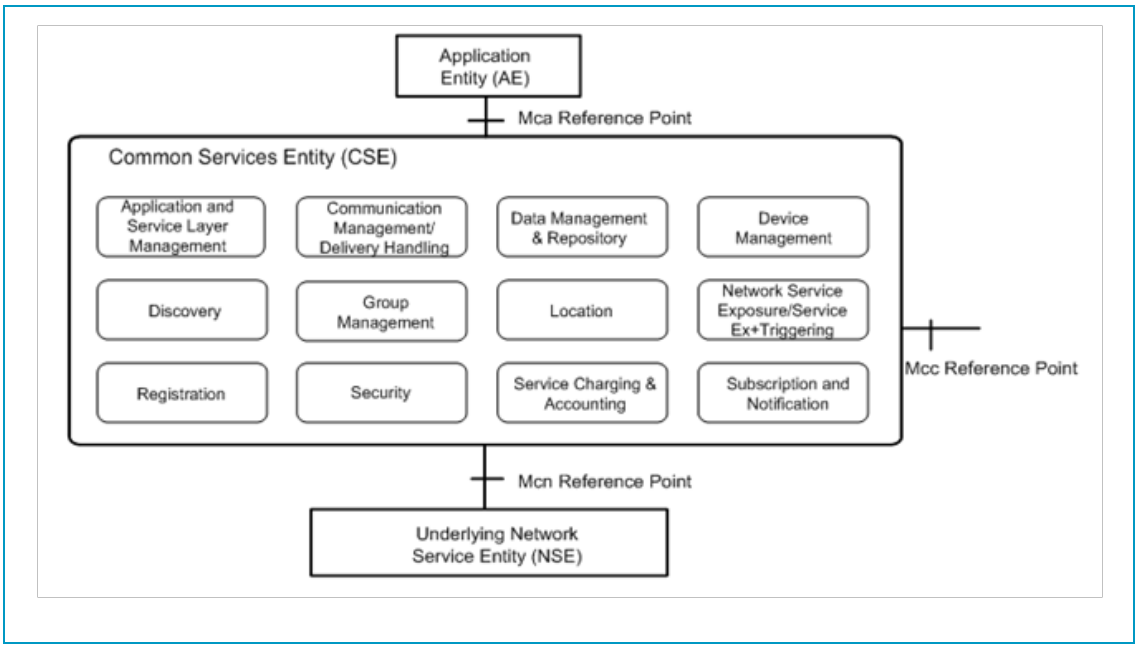
Por otro lado, se puede destacar que muchas de las funcionalidades definidas están relacionadas en ambos sistemas. Sin embargo, la descripción que se hace en el

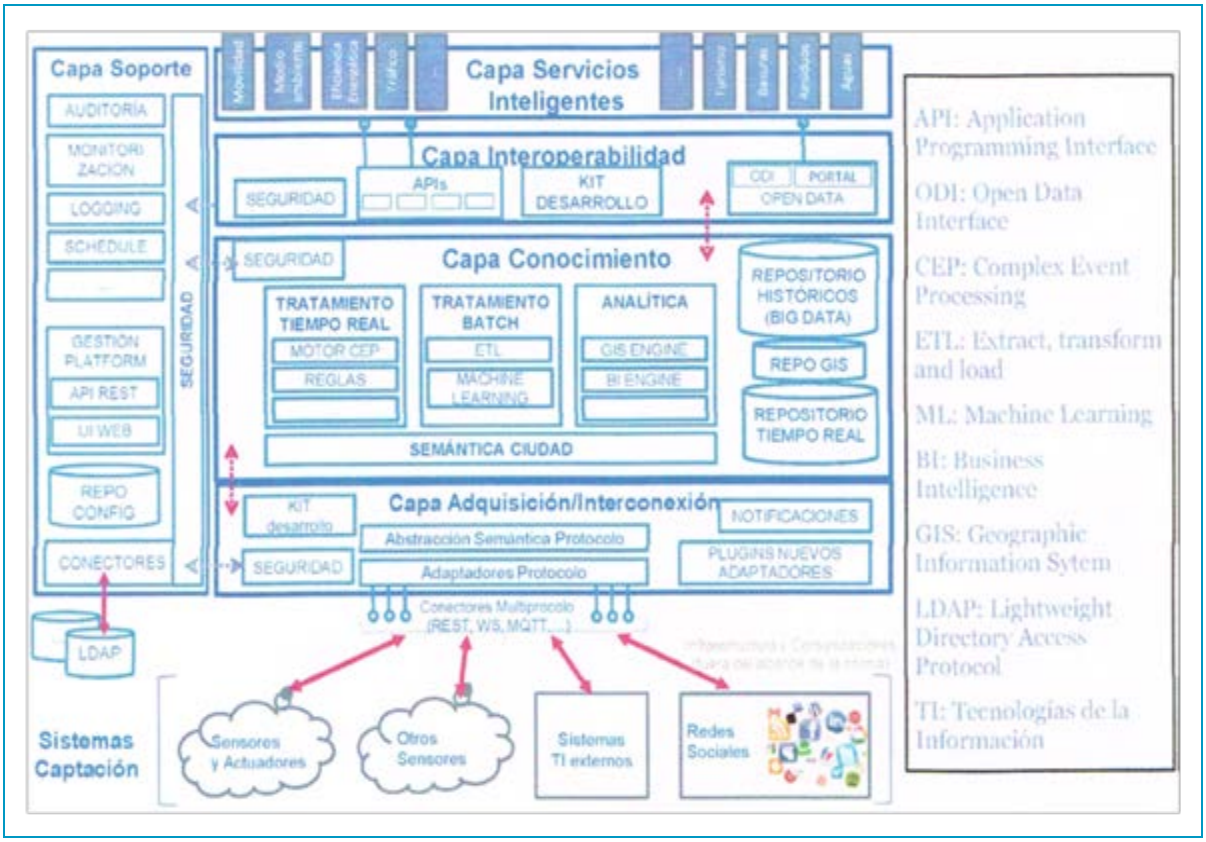
documento UNE, como se ha mencionado anteriormente, se centra en la definición funcional, sin definir el detalle interno de la implementación de esa funcionalidad. Por el contrario, en la norma oneM2M dichas funcionalidades están descritas a un nivel mucho más profundo, por lo que, con el fin de asegurar la interoperabilidad entre sistemas, se deberá considerar lo descrito en el documento normativo TS-0001 del oneM2M.



2. *Estructura de capas y definición de requisitos:*

En la figura siguiente, se detallan las diferentes capas descritas según el estándar oneM2M, así como los diferentes interfaces de relación entre ellas.





Teniendo en cuenta las funcionalidades que se definen como Servicios Comunes (CSE) para el oneM2M y lo que se considera en la UNE, se pueden apreciar las principales diferencias que se establecen en ambos documentos, reflejadas en la siguiente tabla:

oneM2M	UNE
Application and Service Layer Management	Gestión de los servicios inteligentes
Discovery	En la norma UNE no se trata el descubrimiento de recursos
Registration	Funcionalidad de Seguridad (asignación de roles a servicios inteligentes)
Communication Management / Delivery Handling	Funcionalidad de comunicación entre sistemas
Group Management	En la norma UNE no se trata la gestión de grupos
Security	Funcionalidad de Soporte Seguridad
Data Management & Repository	Funcionalidad de repositorio completo y actualizado de información de la ciudad
Location	Funcionalidad de repositorio GIS
Service Charging & Accounting	Funcionalidad de imputación de costes
Device Management	Funcionalidad de gestión de dispositivos
Network Service Exposure / Service Ex+Triggering	Funcionalidad de comunicación entre sistemas
Subscription and Notification	En la norma UNE no se trata la suscripción y notificación

Cómo se ha descrito en los anteriores apartados, en el documento UNE de Plataformas Integrales no se consideran funcionalidades tales como gestión de grupos, suscripción o notificación, que sí están contempladas dentro de la definición del sistema oneM2M.

Realizando una comparación a nivel del modelo de capas, se puede ver cómo gran parte de las funcionalidades definidas por el documento oneM2M están englobadas dentro de las capas de “Adquisición/Interconexión”, “Conocimiento” e “Interoperabilidad” de la arquitectura propuesta por la UNE. Por su parte, en la norma UNE se definen algunas funcionalidades de más alto nivel que no se encuentran descritas en detalle en la

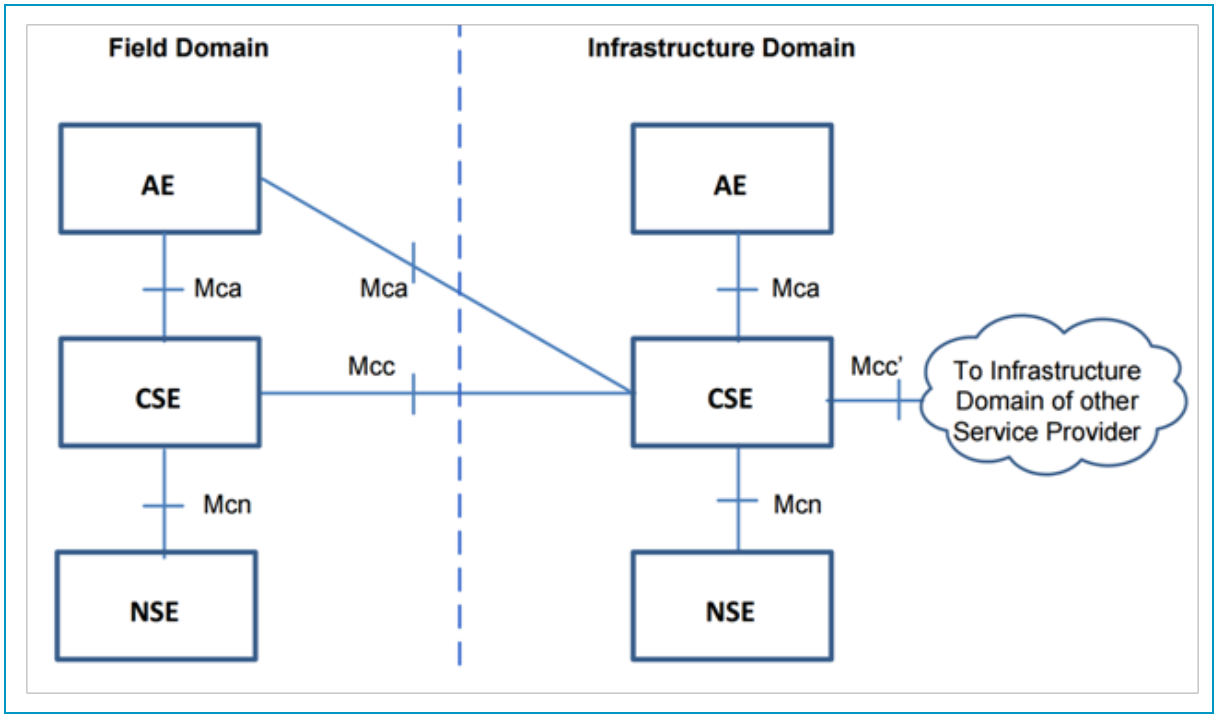
especificación oneM2M, en general más de aplicación especifica a servicios de Gestión de Ciudades, como es el caso de:

- Repositorio Big Data para el acceso a la información tanto histórica como en tiempo real.
- Kit de desarrollo para aplicaciones.
- Portal Open Data utilizado para la implementación de servicios a cliente, entre plataformas, la publicación de datos abiertos o la construcción de Servicios dentro de la Capa de Servicios Inteligentes.
- Módulo de Machine Learning.
- Tratamiento ETL de los datos adquiridos.
- Soporte de tratamiento Batch.
- Análisis a través de procesos BI.
- Funcionalidades de la capa de Soporte: repositorio de configuración de la Plataforma Integral, conectores con repositorios de seguridad tipo LDAP, entorno Web de gestión de la configuración, etc.

3. *Puntos de referencia:*

Con respecto a los puntos de referencia o interfaces, en el sistema oneM2M se definen los siguientes, mostrados en la arquitectura funcional de la figura siguiente:

- Mca: Punto de referencia entre AE y CSE.
- Mcn: Punto de referencia entre NSE y CSE.
- Mcc: Punto de referencia entre dos CSEs.
- Mcc': Punto de referencia entre el CSE y un CSE de otro proveedor de servicios.



En el caso del modelo de capas definido en el documento UNE, no se definen puntos de referencia como tal. (Ver apartado 4.3 de este documento donde se han definido los puntos de referencia en este Estudio).

4. *Interoperabilidad:*

Respecto a la interoperabilidad entre sistemas, aplicaciones y dispositivos, en la norma oneM2M se define completamente la estructura de los recursos y las relaciones entre ellos, los atributos que debe contener cada recurso (y si son de lectura/escritura o solo de lectura o de escritura) y los tipos de recursos hijo que deben contener, datos que no se tienen en cuenta específicamente en la UNE ya que se trata de una especificación de más alto nivel, pero si se recomienda en la UNE el cumplimiento del oneM2M para estos aspectos.

Por otro lado, en la norma UNE no se definen las diferentes operaciones que se pueden ejecutar sobre los recursos, y sí en el documento oneM2M (que permite las operaciones de CREATE (C), RETRIEVE (R), UPDATE (U), DELETE (D), NOTIFY (N)), donde también se define la forma en la que se procesa cada operación para cada recurso y los métodos de direccionamiento de dichos recursos. En la norma UNE no se definen, pero si se recomienda en la UNE el cumplimiento del oneM2M por lo que se debería utilizar la misma estructura de datos, la misma forma de procesar las peticiones y el direccionamiento de los recursos, para evitar así problemas de compatibilidad y una costosa adaptación con el estándar oneM2M y garantizar de esta manera la portabilidad de dispositivos y aplicaciones. Por lo que para garantizar la interoperabilidad, se debería especificar el cumplimiento adicional de oneM2M como obligatorio no como recomendado.

5. *Seguridad:*

En cuanto a la seguridad, se puede comprobar cómo ambos sistemas confluyen en un punto común, un sistema de control de seguridad basado en roles de usuario. La implementación de dicho sistema se basa prácticamente en su totalidad en la asignación de permisos de acceso en función del rol que el usuario tiene dentro del sistema en concreto.

6. *Gestión de dispositivos y comunicaciones:*

En el sistema oneM2M la gestión de dispositivos se hace de forma que se elimina la necesidad de que las aplicaciones desarrolladas basadas en oneM2M (AEs) tengan conocimiento de la tecnología específica de gestión de cada dispositivo o su modelo de datos interno. Para lograr la adaptación y la correcta traducción, se usan los Management Adapters (MA), el cual según la arquitectura de capas de la norma UNE se corresponde totalmente con el adaptador de protocolo de la capa de Adquisición/Interconexión.

Cuando se trata del nodo IN (que se corresponde con la Plataforma Integral de la norma UNE) el Management Adapter de ese nodo está conectado al Management Server (MS) de cada tecnología específica (TR-069, OMA, DM, LWM2M, etc.) para así poder comunicarse con los dispositivos y poder gestionarlos usando el lenguaje específico de cada dispositivo. Este MS es totalmente equivalente a los conectores multiprotocolo de la capa de Adquisición/Interconexión.

Tanto el adaptador de protocolo como los conectores multiprotocolo de la capa de Adquisición/Interconexión no se encuentran detalladamente especificados en la norma UNE, ya que solo se muestran en la vista de capas de la Plataforma Integral y no se profundiza sobre ellos. Para un desarrollo más rápido y disminuir los problemas de

interoperabilidad es recomendable usar el trabajo ya realizado en oneM2M en el Management Adapter para especificar el adaptador de protocolo y el trabajo realizado en el Management Server para especificar los conectores multiprotocolo de la capa de Adquisición/Interconexión de la norma UNE.

Como conclusión,

Ambos estándares son compatibles y complementarios de cara a garantizar la funcionalidad requerida pero para tener la garantía de interoperabilidad es recomendable el cumplimiento de oneM2M por parte de las Plataformas, app y dispositivos de Ciudades Inteligentes

4. METODOLOGÍA DE ANÁLISIS Y CUMPLIMIENTO DE REQUISITOS

Una vez identificados los requisitos que deben cumplir las Plataformas de gestión respecto a las normas de referencia, se hace necesario establecer una metodología de pruebas y análisis del cumplimiento de dichos requisitos para estos sistemas.

4.1. INTRODUCCIÓN A LA METODOLOGÍA DE VALIDACIÓN

Una Metodología de Pruebas es un conjunto de métodos que se aplican durante el proceso de validación o aceptación de un sistema.

Para definir la metodología de pruebas de este proyecto se seguirá el documento ISO/IEC 9646 "Framework and Methodology for Conformance Testing" [26].

Siguiendo esta norma, se ha definido una metodología de pruebas básica para este proyecto en la que se han especificado las siguientes etapas o fases:

Fases de prueba según la ISO/IEC 9646

- *Fase I: Elementos o componentes para ser probados y validados. Su principal objetivo es seleccionar los componentes que van a ser probados y validados posteriormente.*
- *Fase II: Especificaciones de prueba. Una vez que se han decidido los componentes que serán probados y validados, será necesario definir las funcionalidades que deben verificarse durante las pruebas para posteriormente definir todos los casos de prueba necesarios. En esta fase se decidirá la estrategia de test que será aplicada.*
- *Fase III: Definición del plan de pruebas. Se detallará la forma de ejecutar cada uno de los casos de prueba y se definirá el criterio PASA/FALLA que indicará si el resultado de la prueba es satisfactorio o no, en caso de que sea aplicable.*
- *Fase IV: Definición del entorno de pruebas. En esta fase se describen las condiciones en las que deben realizarse las pruebas.*
- *Fase V: Ejecución del plan de pruebas. Los resultados se deben recoger en una plantilla que recoja como mínimo información acerca del objetivo de la prueba, el elemento testeado, los pasos a seguir para realizar la prueba, y el resultado.*

En resumen, una vez definidos los estándares, los pasos siguientes para la definición de la metodología son:

- Definir el catálogo de capacidades a valorar
- Especificar el conjunto de casos de pruebas
- Definir la estructura de los casos de prueba
- Especificar los propósitos de prueba (TP)
- Definir el procedimiento y condiciones de prueba

4.1.1. DEFINICIONES

A continuación se recogen una serie de definiciones de interés para la comprensión de definición de la metodología.

- **Pruebas de conformidad:** garantizan que un producto implementa correctamente el estándar y es capaz intercambiar información con otra aplicación utilizando un protocolo o conjunto de protocolos conocidos.
- **Pruebas de interoperabilidad:** se realizan por medio de dispositivos de diferentes fabricantes y conexión entre ellos, ya sea manual o automáticamente, de acuerdo con escenarios basados en un protocolo estándar.
- **DUT:** dispositivo bajo prueba (Device under Test) es una combinación de los elementos software y/o hardware que implementan la funcionalidad del estándar e interactúan con otros DUTs a través de los puntos de referencia.

- **Interoperabilidad:** capacidad de dos sistemas de interoperar usando el mismo protocolo de comunicación.

- **Función de interfuncionamiento (IWF):** traducción de un protocolo en otro de manera que dos sistemas que usan diferentes protocolos de comunicación puedan interoperar.

- **Equipo cualificado (QE):** grupo de uno o más dispositivos que han sido certificados, mediante un ensayo riguroso y bien definido, para interoperar con otro equipo. Una vez que un DUT se haya probado con éxito contra un QE, puede ser considerado un QE sí mismo.

- **Caso de prueba (TC):** especificación de las acciones requeridas para alcanzar un propósito específico de prueba. Las acciones pueden estar definidas en lenguaje natural, para operación manual, o en un lenguaje legible por máquinas (como TTCN-3), para la ejecución automática.

- **Propósito de prueba (TP):** descripción del objetivo bien definido de la prueba, centrándose en un solo requisito o un sistema de requisitos relacionados.

- **Implementation Conformance Statement (ICS):** declaración hecha por el suministrador de la muestra a probar, especificando las capacidades que implementa y no implementa el sistema.

- **ICS proforma:** documento, en forma de cuestionario, que cuando se completa para un sistema se convierte en un ICS.

- **Implementation eXtra Information for Testing (IXIT):** checklist que contiene información adicional a la proporcionada en el ICS relativa al DUT y su entorno de pruebas, y que permitirán al laboratorio de pruebas la ejecución de los ensayos.

- **IXIT proforma:** documento, en forma de cuestionario, que cuando se completa para un sistema se convierte en un IXIT.

- **Implementation under Test (IUT):** es una implementación del protocolo que puede ser considerada como un objeto para ser medido.

4.1.2. PRUEBAS DE CONFORMIDAD

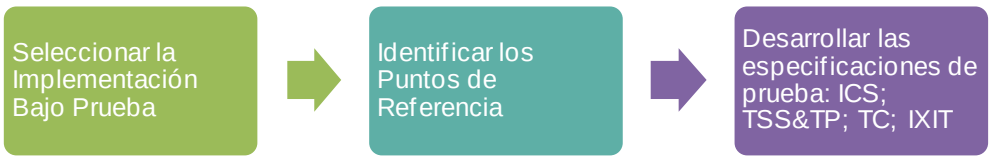
Las pruebas de conformidad demuestran que **un producto implementa adecuadamente o no un protocolo estándar particular**, es decir, verifica que se cumplen los requisitos establecidos en las normas. Normalmente se utiliza un sistema automático de medida para realizar la verificación.

Siguiendo los pasos definidos anteriormente, la metodología empieza con la categorización, de forma tabular, de las funciones y opciones a ser medidas, es decir el primer paso es definir el ICS (Implementation Conformance Statement) para el estándar correspondiente, para ello se listarán todas las capacidades soportadas por los sistemas a validar.

El paso siguiente es extraer los requisitos de la especificación. Posteriormente para cada requisito se identifican los casos de prueba a realizar, que se agruparán de manera estructurada (TSS).

Para cada identificador, se asocia un TP (propósito de test), finalmente se escribe un TC (Caso de prueba) detallado para cada TP.

En resumen la metodología a aplicar es la siguiente:



Estos son los pasos que se siguen para ambos estándares de referencia en los apartados siguientes de este documento.

Seleccionar la Implementación Bajo Prueba

La Implementación bajo prueba o IUT, es una implementación del protocolo que puede ser considerada como un objeto para ser medido, es decir, se verificarán los requisitos de una especificación sobre ese objeto que lo implementa.

Identificación de los puntos de Referencia

Los puntos de referencia son las interfaces de una IUT a las que habrá que conectarse para verificar la conformidad con el protocolo.

ICS

El propósito de un ICS es identificar las funciones estandarizadas que debe soportar un IUT y cuales son opcionales o condicionadas a la presencia de otras funciones.

Se puede utilizar como un documento que identifica las funciones declaradas por el suministrador de la IUT a probar. Normalmente se presentan de forma tabular.

Usualmente el documento que recoge los ICS se estructura de la siguiente forma:

- Guía para completarlo
- Identificación de la implementación (fabricante, nombre, versión, etc.)
- Identificación de la especificación
- Declaración de conformidad (en forma de cuestionario)

TSS&TP

El Propósito de Prueba o "TP" es una descripción clara del objetivo de la prueba. Puede estar relacionado con uno o varios requisitos establecidos en la especificación.

La organización de los TPs en grupos es lo que se conoce como TSS o Estructura del conjunto de prueba.

TC

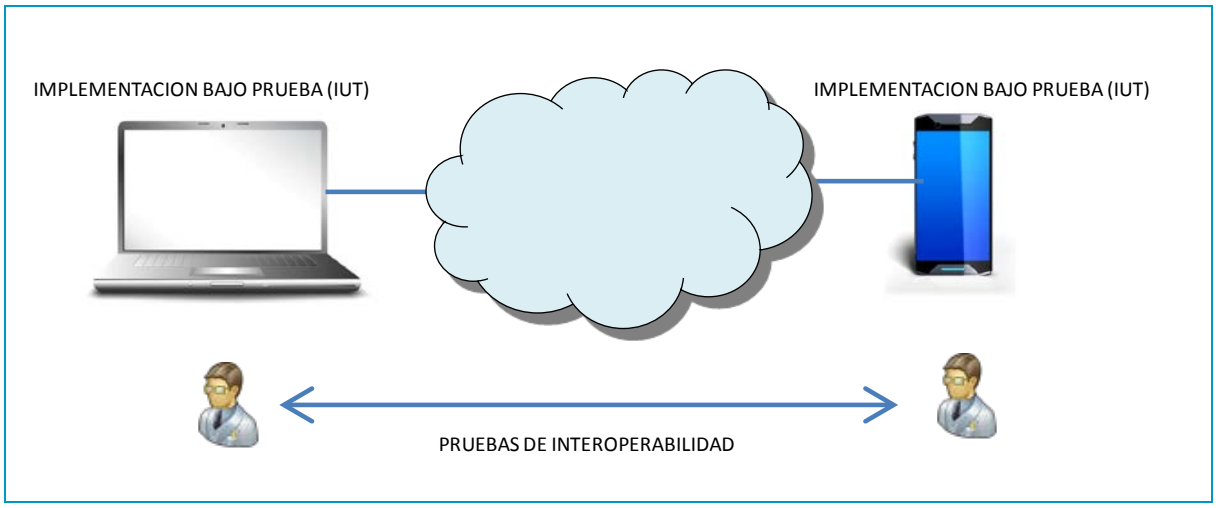
Para cada TP se define el TC (caso de prueba) correspondiente, que consiste en especificar los procedimientos y las acciones requeridas para alcanzar el propósito del test y realizar la verificación de los requisitos asociados. Para ello, habrá que seguir el flujo de los protocolos establecidos en las especificaciones y emular el comportamiento del sistema con el que interactúa el IUT.

IXIT

Es la información adicional de los IUT a los ICS y que se considera necesaria para poder ejecutar los Casos de prueba. Pueden ser ciertos parámetros (direcciones, temporizadores, etc.) o especificidades relacionadas con el comportamiento del IUT durante las pruebas. El documento que recoge esta información también es suministrado por el proveedor de la muestra para ensayo.

4.1.3. PRUEBAS DE INTEROPERABILIDAD

Las pruebas de interoperabilidad demuestran la interactuación entre dos o más productos. Se comprueba la funcionalidad extremo a extremo, recogida en las especificaciones, entre varios dispositivos o sistemas, por lo que el sistema bajo prueba debe estar compuesto por varios dispositivos provenientes de diferentes fabricantes.

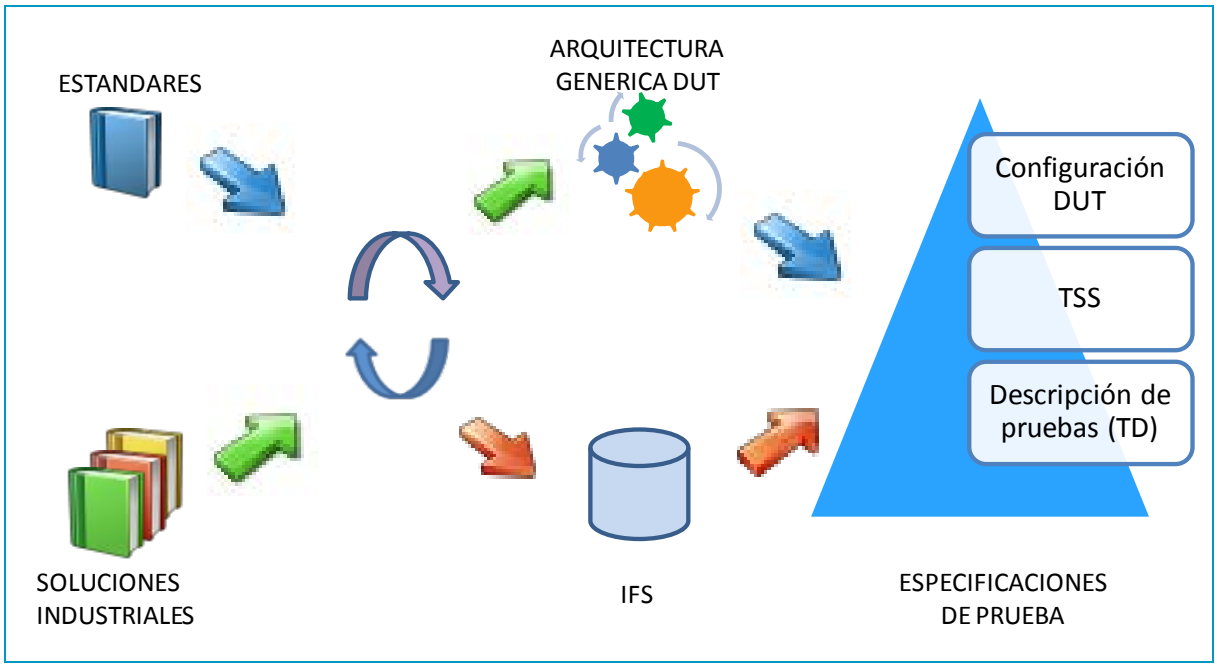


A la hora de definir las pruebas de interoperabilidad es imprescindible tener en cuenta lo siguiente:

- Las pruebas de interoperabilidad deben ser ejecutadas en aquellos interfaces que ofrecen de manera natural, es decir no hay que definir interfaces con el único fin de realizar pruebas.
- Las pruebas de interoperabilidad son funcionales, no a nivel de protocolo.
- Las pruebas serán ejecutadas sobre interfaces funcionales, como las interfaces hombre-máquina, interfaces de servicio y APIs.

Al ser ejecutadas sobre interfaces funcionales, los casos de prueba solo contemplarán el comportamiento funcional de los sistemas a probar. Los componentes básicos para establecer un marco de pruebas de interoperabilidad son:

- Definición de la arquitectura de pruebas
- Desarrollo de las especificaciones de prueba de interoperabilidad que incluye:
    - Definición de la arquitectura genérica de un Sistema bajo Prueba
    - Especificación de la Configuración de Pruebas
    - Identificación de las Funciones Interoperables
    - Desarrollo de las Descripciones de Prueba



Arquitectura de Pruebas

Los conceptos básicos a tener en cuenta para definir las especificaciones de prueba de interoperabilidad son:

- Sistema bajo Prueba: El sistema bajo prueba estará compuesto por varios Dispositivos bajo Prueba (DUT) de diferentes fabricantes. Es posible que el sistema bajo prueba presente diferentes configuraciones dependiendo del DUT con el que va a interoperar.

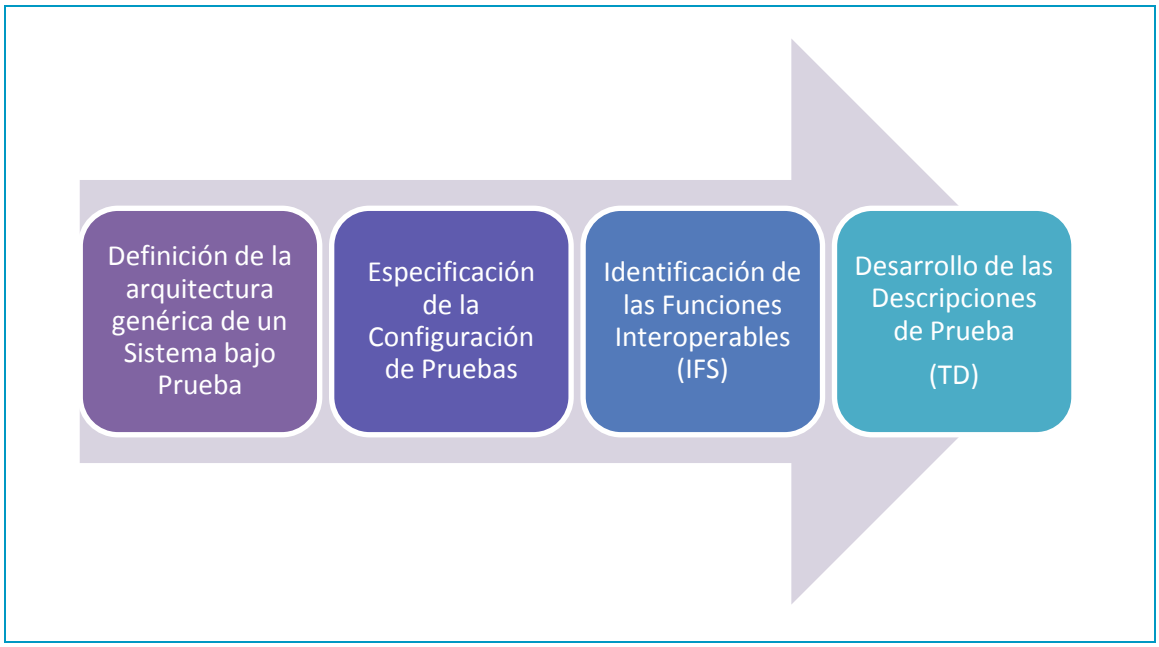
- Dispositivo bajo Prueba (DUT): Los dispositivos bajo prueba, en este caso, pueden ser combinaciones de hardware y/o software que implementen la funcionalidad referida en el estándar y que interactúan con otros dispositivos a través de los puntos de referencia.

- Test Interfaces: Son interfaces a través de las cuales se ejecutan las pruebas. Se accede a ellas a través de los drivers de test para estimular y verificar el comportamiento del sistema. Normalmente estas interfaces serán interfaces de usuario (línea de comandos, interfaces web, etc.) o APIs.

- Test Environment: Es la combinación de equipos y procedimientos que posibilitan la ejecución de las pruebas de interoperabilidad. Tiene los elementos necesarios para asegurar la selección, ejecución e interpretación de los resultados, la coordinación y sincronización de las acciones y los mecanismos de loggin y monitorización. Está formado por la descripción detallada de la prueba y por los test drivers, que son los encargados de ejecutar, sobre las interfaces definidas, los pasos especificados en la descripción de la prueba

Especificaciones de Prueba

Los pasos para desarrollar las especificaciones de prueba de interoperabilidad son:



1. La **arquitectura** genérica debe ser capaz de recoger cualquier configuración que pueda presentar un sistema bajo prueba. El punto de partida suele ser la propia arquitectura funcional definida en el estándar, en combinación con las implementaciones que se estén realizando de dichos bloques funcionales. Generalmente, se especifica como un diagrama donde se identifican: el dispositivo bajo prueba y los bloques funcionales que incluye, las rutas de comunicación entre DUTs y los protocolos, APIs y/o modelos de datos que se usan para comunicar los DUTs.

2. La arquitectura de **configuración** de las pruebas es una descripción de entidades lógicas, sus interfaces y las comunicaciones relacionadas con la prueba. Estará principalmente compuesta por los siguientes elementos:

    - SUT (Sistema bajo Prueba): Conjunto de DUTs que contemplan el software, hardware y dispositivos (sensores, etc.) necesarios para ejecutar las pruebas.

    - Test bed control module: Se encarga de la gestión del sistema de pruebas (test bed) realizando sincronización, configuración, control y ejecución de los diferentes elementos, así como de la recopilación de resultados, y algunos caso (herramientas automáticas) del asignar el veredicto de la prueba.

    - Test stimulation environment: Se encarga de generar los estímulos adecuados en cada prueba.

    - Monitor: Se encarga de recoger información relevante intercambiada entre DUTs.

    - Red: Se consideran dos tipos la de datos y la de control.

3. La estructura de una declaración de las características de interoperabilidad (**IFS**) es similar a la de los ICS. Su propósito es identificar las funciones especificadas en el estándar base que debe soportar una implementación, aquellas que son opcionales y aquellas que están condicionadas a la existencia de otras funciones.

   Como con los ICS, un IFS proforma sirve para que el solicitante del ensayo identifique qué funciones soportará un DUT.

   El punto de partida lógico en el desarrollo de IFS son los ICS, que identifican claramente las opciones y condiciones que se aplican al protocolo a ser probado.

4. La descripción de la prueba (**TD**) consiste en una descripción detallada del proceso que va a verificar una o más funcionalidades de una implementación.

   Los elementos mínimos que debe incluir son:

Identifier	Identificador
Objective	Descripción corta del objetivo de la prueba
References	La referencia indica las cláusulas de las especificaciones de referencia en las cuales se expresa el requisito a verificar
Applicability	La lista de funciones y capacidades que debe soportar el SUT para que la prueba pueda ser ejecutada
Configuration or Architecture	Lista de equipos requeridos para desplegar la arquitectura y la configuración de la prueba
Pre-Test Conditions	Lista de precondiciones que debe cumplir el SUT incluyendo información sobre la configuración de los equipos
Test Sequence	Lista de operaciones y observaciones a ejecutar durante la prueba

4.2. METODOLOGÍA DE VALIDACIÓN PARA TS-0001 (ONEM2M)

El grupo TST de oneM2M es el encargado de la definición de la metodología de validación frente al estándar oneM2M. Sus resultados se recogen en diferentes borradores de documentos, todavía en ejecución, como son:

- TS 0013 Interoperability Testing [17]
- TS 0015 Testing Framework [18]
- TS 0017 Implementation Conformance Statements [19]
- TS 0018 Test Suite Structure and Test Purposes [20]

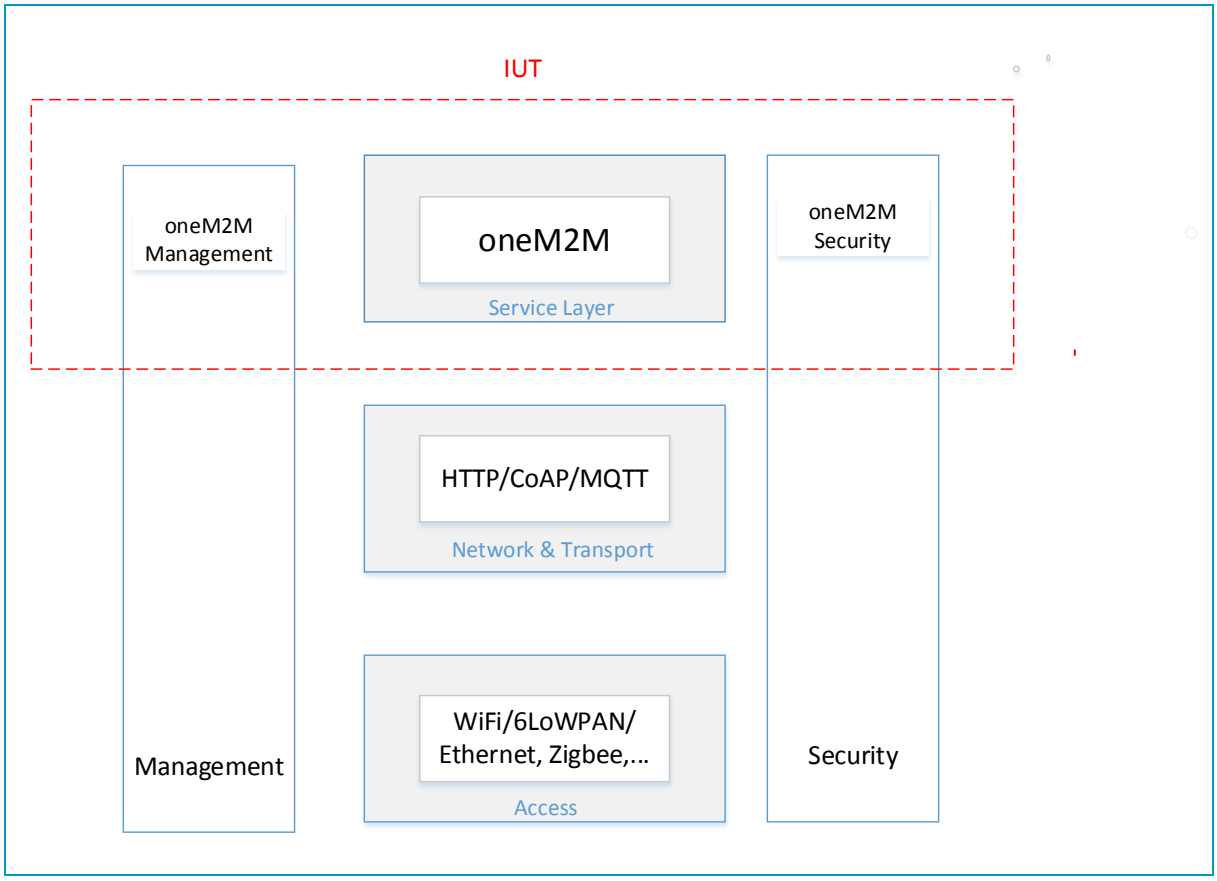
Todavía a la fecha de elaboración de este documento queda bastante trabajo que hacer dentro del Grupo TST de oneM2M para completar las Especificaciones de Prueba completas, que posteriormente serán publicadas, por lo que este apartado se incluye solo a modo informativo ya que podrá ir variando a lo largo del tiempo hasta que existan versiones aprobadas y publicadas de los documentos de referencia.

A continuación se recoge lo desarrollado hasta el momento por el grupo de trabajo para las pruebas de conformidad.

4.2.1. PRUEBAS DE CONFORMIDAD TS-0001

Conformidad: Implementación bajo prueba

Como ejemplo de una implementación (IUT) de la arquitectura oneM2M se puede considerar la siguiente (como se recoge en el borrador TS-0015 [18] del oneM2M):



En función del tipo de nodo y las interfaces definidas en la arquitectura oneM2M, los nodos a testear son:

IUT (nodo)	Entidad	Interfaces
ASN	Application Entity (AE)	Mca
	Common Services Entity (CSE)	Mca, Mcc, Mcn
ADN	Application Entity (AE)	Mca
MN	Application Entity (AE)	Mca
	Common Services Entity (CSE)	Mca, Mcc, Mcn
IN	Application Entity (AE)	Mca
	Common Services Entity (CSE)	Mca, Mcc, Mcn, Mcc', Mch
ASN/MN/IN	Network Services Entity (NSE)	Mcn

Este proyecto, como se ha indicado anteriormente, se centra en los nodos tipo IN, marcados en azul.

Conformidad: Puntos de referencia

A continuación se muestran los puntos de referencia (Reference Point – RP) que habrá que testear para verificar el cumplimiento de los protocolos definidos oneM2M.

Identificador RP	Tipo RP	Nodo / entidad	Nodo / entidad
RP-oneM2M-1	Mca	ASN-AE	ASN-CSE
RP-oneM2M-2	Mca	MN-AE	MN-CSE
RP-oneM2M-3	Mca	IN-AE	IN-CSE
RP-oneM2M-4	Mca	ADN-AE	IN-CSE
RP-oneM2M-5	Mca	ADN-AE	MN-CSE
RP-oneM2M-6	Mcc	ASN-CSE	IN-CSE
RP-oneM2M-7	Mcc	ASN-CSE	MN-CSE
RP-oneM2M-8	Mcc	MN-CSE	MN-CSE
RP-oneM2M-9	Mcc	MN-CSE	IN-CSE
RP-oneM2M-10	Mcn	ASN-CSE	NSE
RP-oneM2M-11	Mcn	MN-CSE	NSE
RP-oneM2M-12	Mcn	IN-CSE	NSE
RP-oneM2M-13	Mcc'	IN-CSE	IN-CSE'
RP-oneM2M-14	Mch	IN-CSE	Charging Server

Conformidad: ICS

Según la última versión del borrador disponible en la elaboración de este informe [19], los ICS identificados son los siguientes:

Tipo de nodo soportado por la IUT

Item	Node Type
1	ASN-CSE
2	MN-CSE
3	IN-CSE
4	ASN-AE
5	MN-AE
6	IN-AE
7	ADN-AE

Se debe seleccionar uno de ellos para cada ensayo. De cara a este proyecto solo tienen relevancia los marcados en azul.

Declaración de capacidades

Item	Capability
1	Registration
2	Data Management
3	Subscription and Notification
4	Group Management
5	Discovery
6	Location Management
7	Device Management
8	Communication Management and Delivery Handling

Puntos de referencia

Node Role / Reference Point	ASN-CSE	MN-CSE	IN-CSE	ASN-AE	MN-AE	IN-AE	ADN-AE
Mca	M	M	M	M	M	M	M
Mcc	M	M	M	N/A	N/A	N/A	N/A
Mcn	M	M	M	N/A	N/A	N/A	N/A
Mcc	N/A	N/A	M	N/A	N/A	N/A	N/A

M: Mandatory (obligatorio)

N/A: No aplica

Tipos de respuestas aceptadas por CSE

Item	Response Type	
1	Blocking	
2	Non-Blocking	Synchronous
		Asynchronous

Conformidad: TSS&TP

Los grupos y subgrupos de Casos de prueba definidos actualmente en los borradores de los documentos [20] del oneM2M son:

- Group 1: ASN-CSE
  - Group 1.1: Originator
    - Subgroup 1.1.1: Registration
    - Subgroup 1.1.2: Data Management
    - Subgroup 1.1.3: Subscription/Notification
    - Subgroup 1.1.4: Group Management
    - Subgroup 1.1.5: Device Management

        - Subgroup 1.1.6: Announcement
        - Subgroup 1.1.7: Communication Management/Delivery Handling
        - Subgroup 1.1.8: Security
    - Group 1.2: Receiver
        - Subgroup 1.2.1: Registration
        - Subgroup 1.2.2: Resource Management
        - Subgroup 1.2.3: Data Management
        - Subgroup 1.2.4: Subscription/Notification
        - Subgroup 1.2.5: Group Management
        - Subgroup 1.2.6: Location Management
        - Subgroup 1.2.7: Device Management
        - Subgroup 1.2.8: Announcement
        - Subgroup 1.2.9: Communication Management/Delivery Handling
        - Subgroup 1.2.10: Security
- Group 2: MN-CSE
    - Group 2.1: Originator
        - Subgroup 2.1.1: Registration
        - Subgroup 2.1.2: Resource Management
        - Subgroup 2.1.3: Data Management
        - Subgroup 2.1.4: Subscription/Notification
        - Subgroup 2.1.5: Group Management
        - Subgroup 2.1.6: Location Management
        - Subgroup 2.1.7: Device Management
        - Subgroup 2.1.8: Announcement
        - Subgroup 2.1.9: Communication Management/Delivery Handling
        - Subgroup 2.1.10: Security
    - Group 2.2: Receiver
        - Subgroup 2.2.1: Registration
        - Subgroup 2.2.2: Resource Management
        - Subgroup 2.2.3: Data Management
        - Subgroup 2.2.4: Subscription/Notification
        - Subgroup 2.2.5: Group Management
        - Subgroup 2.2.6: Location Management
        - Subgroup 2.2.7: Device Management
        - Subgroup 2.2.8: Announcement
        - Subgroup 2.2.9: Communication Management/Delivery Handling
        - Subgroup 2.2.10: Security
- **Group 3: IN-CSE**
    - **Group 3.1: Originator**
        - **Subgroup 3.1.1: Subscription/Notification**
        - **Subgroup 3.1.2: Communication Management/Delivery Handling**
    - **Group 3.2: Receiver**
        - **Subgroup 3.2.1: Registration**
        - **Subgroup 3.2.2: Resource Management**
        - **Subgroup 3.2.3: Data Management**
        - **Subgroup 3.2.4: Subscription/Notification**
        - **Subgroup 3.2.5: Group Management**
        - **Subgroup 3.2.6: Location Management**
        - **Subgroup 3.2.7: Device Management**
        - **Subgroup 3.2.8: Announcement**
        - **Subgroup 3.2.9: Communication Management/Delivery Handling**
        - **Subgroup 3.2.10: Security**
- Group 4: ASN-AE
    - Group 4.1: Originator
        - Subgroup 4.1.1: Registration
        - Subgroup 4.1.2: Resource Management

        - Subgroup 4.1.3: Data Management
        - Subgroup 4.1.4: Subscription/Notification
        - Subgroup 4.1.5: Group Management
        - Subgroup 4.1.6: Location Management
        - Subgroup 4.1.7: Device Management
        - Subgroup 4.1.8: Announcement
        - Subgroup 4.1.9: Communication Management/Delivery Handling
        - Subgroup 4.1.10: Security
- Group 5: MN-AE
    - Group 5.1: Originator
        - Subgroup 5.1.1: Registration
        - Subgroup 5.1.2: Resource Management
        - Subgroup 5.1.3: Data Management
        - Subgroup 5.1.4: Subscription/Notification
        - Subgroup 5.1.5: Group Management
        - Subgroup 5.1.6: Location Management
        - Subgroup 5.1.7: Device Management
        - Subgroup 5.1.8: Announcement
        - Subgroup 5.1.9: Communication Management/Delivery Handling
        - Subgroup 5.1.10: Security
- **Group 6: IN-AE**
    - **Group 6.1: Originator**
        - **Subgroup 6.1.1: Registration**
        - **Subgroup 6.1.2: Resource Management**
        - **Subgroup 6.1.3: Data Management**
        - **Subgroup 6.1.4: Subscription/Notification**
        - **Subgroup 6.1.5: Group Management**
        - **Subgroup 6.1.6: Location Management**
        - **Subgroup 6.1.7: Device Management**
        - **Subgroup 6.1.8: Announcement**
        - **Subgroup 6.1.9: Communication Management/Delivery Handling**

De interés para esté proyecto serían sólo los nodos tipo IN, resaltados en negrita.

Actualmente tanto los TC como los IXIT están pendientes de desarrollo en el grupo de trabajo TST de oneM2M.

4.2.2. PRUEBAS DE INTEROPERABILIDAD TS-0001

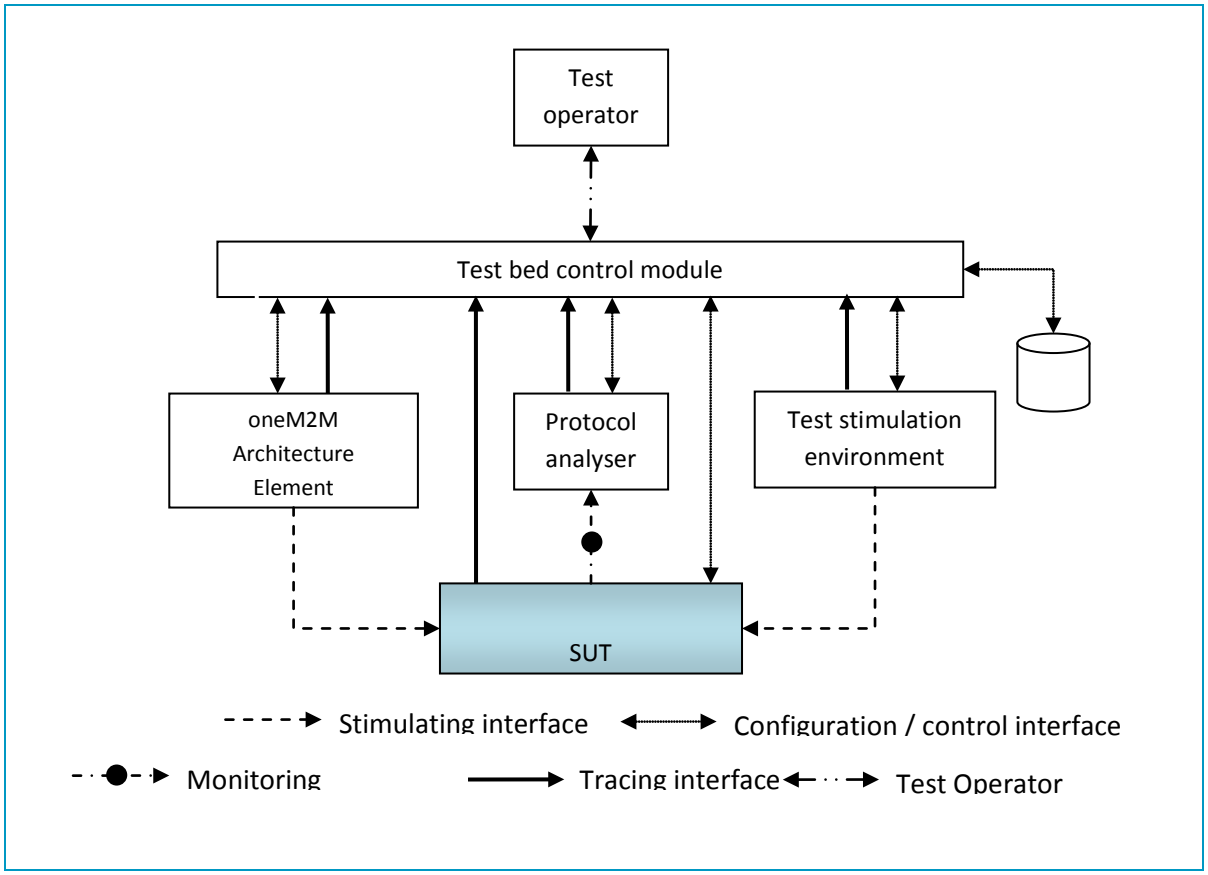
Interoperabilidad: Arquitectura

El grupo de trabajo TST de oneM2M está desarrollando el documento TS-0013 “Interoperability Testing” [17], actualmente en borrador.

El objetivo del TS-0013 [17] es definir las pruebas funcionales extremo a extremo para las entidades de aplicación y servicios comunes a través de las interfaces Mca y Mcc.

En este caso, los sistemas bajo prueba son un conjunto de nodos oneM2M.

La arquitectura de pruebas definida es la siguiente:



Interoperabilidad: Configuración de Prueba

Los requisitos que deben cumplir los nodos para ser probados son:

- Poder deshabilitar la seguridad
- Los nombres de los recursos deben estar pre-cargados, salvo para aquellos que se asignan automáticamente por el hosting CSE.
- Después de cada "delete" de un recurso, el usuario chequeará que realmente se ha borrado.
- Salvo que se especifique lo contrario, todas las aplicaciones tendrán los accesos adecuados para gestionar recursos de un CSE.

Se han definido 9 configuraciones para las pruebas de interoperabilidad disponibles en el documento referido del grupo de trabajo TST.

Interoperabilidad: IFS

Los IFS definidos coinciden con los ICS definidos para las pruebas de conformidad a las que se añaden las siguientes:

- NH: No hop: a medir en el punto de referencia Mca
- NB: Non blocking
- SH: Single hop. Gestión de recursos remotos Mca+Mcc
- MH: Multi hop
- Binding protocol: http, CoAP, MQTT

Interoperabilidad: TD

Los casos de prueba de interoperabilidad identificados hasta el momento en oneM2M [17] son:

Nb	Procedure / Resource	TD ID	TD Description
1	CSEBase Management	TD_M2M_NH_01	AE retrieves the CSEBase resource
2	RemoteCSE	TD_M2M_NH_02	Registree CSE registers to Registrar CSE
3		TD_M2M_NH_03	Registree CSE retrieves RemoteCSE from Registrar CSE
4		TD_M2M_NH_04	Registree CSE updates RemoteCSE from Registrar CSE
5		TD_M2M_NH_05	Registree CSE deletes RemoteCSE from Registrar CSE
6	Application Entity	TD_M2M_NH_06	AE registers to its registrar CSE via an AE Create Request
7		TD_M2M_NH_07	AE retrieves <AE> resource via an AE Retrieve Request
8		TD_M2M_NH_08	AE updates attribute in <AE> resource via an AE Update Request
9		TD_M2M_NH_09	AE de-registers by deleting <AE> resource via an AE Delete Request
10	Container	TD_M2M_NH_10	AE creates a container resource in registrar CSE via a container Create Request
11		TD_M2M_NH_11	AE retrieves information of a container resource via a container Retrieve Request
12		TD_M2M_NH_12	AE updates attribute in application resource via a container Update Request
13		TD_M2M_NH_13	AE deletes a specific container resource via a container Delete Request
14	ContentInstance	TD_M2M_NH_14	AE adds a contentInstance resource <contentInstance> to a specific container in Registrar CSE via a contentInstance Create Request
15		TD_M2M_NH_15	AE retrieves information of a contentInstance resource via a container Retrieve Request
17		TD_M2M_NH_17	AE deletes contentInstance resource via a container Delete Request
18	Discovery	TD_M2M_NH_18	AE discovers resources residing in Registrar CSE
19		TD_M2M_NH_19	AE discovers accessible resources residing in Registrar CSE using the label filter criteria
20		TD_M2M_NH_20	AE discovers accessible resources residing in Registrar CSE limiting the number of matching resources to the specified value.
21		TD_M2M_NH_21	AE discovers accessible resources residing in Registrar CSE using multiple Filter Criteria
22	Subscription	TD_M2M_NH_22	AE creates a subscription to Application Entity resource via subscription Create Request
23		TD_M2M_NH_23	AE retrieves information about a subscription via subscription Retrieve Request such as expirationTime, labels, etc…
24		TD_M2M_NH_24	AE updates information about a subscription via subscription Retrieve Request
25		TD_M2M_NH_25	AE cancels subscription via an subscription Delete Request

26	AccessControlPolicy	TD_M2M_NH_26	AE creates an accessControlPolicy resource
27		TD_M2M_NH_27	AE retrieves accessControlPolicy resource
28		TD_M2M_NH_28	AE updates attribute in accessControlPolicy resource
29		TD_M2M_NH_29	AE deletes accessControlPolicy resource
30		TD_M2M_NH_30	AE delete request is rejected due to accessControlPolicy
31	Group	TD_M2M_NH_31	AE creates a group resource
32		TD_M2M_NH_32	AE retrieves group resource
33		TD_M2M_NH_33	AE updates attribute in group resource
34		TD_M2M_NH_34	AE deletes group resource
35	Node	TD_M2M_NH_35	AE creates a node resource
36		TD_M2M_NH_36	AE retrieves node resource
37		TD_M2M_NH_37	AE updates attribute in node resource
38		TD_M2M_NH_38	AE deletes node resource
39	PollingChannel	TD_M2M_NH_39	AE creates a <pollingChannel> resource in registrar CSE via a Create Request
40		TD_M2M_NH_40	AE retrieves information of a pollingChannel resource via a Retrieve Request
41		TD_M2M_NH_41	AE updates attribute in pollingChannel resource via a Update Request
42		TD_M2M_NH_42	AE deletes a pollingChannel resource via a Delete Request
43		TD_M2M_NH_43	AE retrieves information of a pollingChannel resource via a Retrieve Request
44	FanoutPoint	TD_M2M_NH_44	AE creates a <contentInstance> resource in each group member
45		TD_M2M_NH_45	AE retrieves the <container> resource from in each group member
46		TD_M2M_NH_46	AE updates an <container> resource of each member resource
47		TD_M2M_NH_47	AE deletes a <container> ofeach member
48	Notification	TD_M2M_NH_48	AE receives a notification request from the HOST CSE

49	Synchronous request	TD_M2M_NB_01	AE creates a container resource using non blocking synchronous request in registrar CSE.
50		TD_M2M_NB_02	AE retrieves a Container resource using non blocking synchronous request in registrar CSE.
51		TD_M2M_NB_03	AE updates a Container resource using non blocking synchronous request in registrar CSE.
52		TD_M2M_NB_04	AE deletes a Container resource using non blocking synchronous request.
53	Asynchronous request	TD_M2M_NB_05	AE creates a container resource using non blocking asynchronous request
54		TD_M2M_NB_06	AE retrieves a Container resource using non blocking asynchronous request
55		TD_M2M_NB_07	AE updates a Container resource using non blocking asynchronous request
56		TD_M2M_NB_08	AE deletes a Container resource using non blocking asynchronous request
57	Retargeting	TD_M2M_SH_01	AE creates a remote <Resource> resource
58		TD_M2M_SH_02	AE retrieves a remote <Resource> resource
59		TD_M2M_SH_03	AE updates a remote <Resource> resource
60		TD_M2M_SH_04	AE delete a remote <Resource> resource
61	<mgmtObj>	TD_M2M_SH_05	AE creates a <mgmtObj> resource
62		TD_M2M_SH_06	AE updates a <mgmtObj> resource
63		TD_M2M_SH_07	AE retrieves a <mgmtObj> resource
64		TD_M2M_SH_08	AE deletes a <mgmtObj> resource

Actualmente se han desarrollado todos estos casos de prueba. A continuación, a modo de ejemplo, se muestra el procedimiento para uno de los casos de prueba desarrollados:

Interoperability Test Description			
Identifier:			TD_M2M_NH_01
Objective:			AE retrieves the CSEBase resource
Configuration:			M2M_CFG_01
References:			[1] 10.2.3.2 [2] 7.3.2
Pre-test conditions:			• CSEBase resource has been automatically created in CSE
Test Sequence			
Step	**RP**	**Type**	**Description**
1		Stimulus	AE is requested to send a retrieve Request to CSE CSE with name {CSEBaseName}

Interoperability Test Description			
2	Mca	PRO Check Primitive	Operation (op) = 2 (Retrieve) To (to) = Resource-ID of requested <CSEBase> resource, assumed CSE-relative here From (from) = AE-ID of request originator Request Identifier (rqi) = (token-string)
		PRO Check HTTP	Sent GET request contains • Request method = GET • Request-Target:{CSEBaseName} • Host: Host Address of registrar CSE • X-M2M-RI: value of rqi primitive parameter • X-M2M-Origin: AE-ID • Payload: empty
		PRO Check CoAP	Sent GET request contains • Method: 0.01 (GET) • Uri-Host: Registrar CSE host • Uri-Port: Registrar CSE port • Uri-Path: <CSEBase>
		PRO Check MQTT	Sent a MQTT PUBLISH protocol packet to the request topic "/oneM2M/req/<SP-Relative-AE-ID>/<Registrar CSE-ID>" • Payload: op = 2 to = <CSEBase> fr = <AE-ID> rqi = <Request ID>
3	Mca	PRO Check Primitive	• Response Status Code (rsc) = 2000 (OK) • Request Identifier (rqi) = same string as received in request message Content (pc) = Serialized Representation of <CSEBase> resource
		PRO Check HTTP	Registrar CSE sends response containing: • Status Code = 200 • X-M2M-RSC: 2000 • X-M2M-RI: value of rqi primitive parameter • Content-Type; application/vnd.onem2m-res+xml or application/vnd.onem2m-res+json • Content-Length = size of payload in the message body in bytes • Payload: Serialized Representation of <CSEBase> resource
		PRO Check CoAP	Registrar sends response containing: • Response Code = 2.05 • Payload: <CSEBase> resource
		PRO Check MQTT	Sent a MQTT PUBLISH protocol packet to the response topic "/oneM2M/resp/<SP-Relative-AE-ID>/<Registrar CSE-ID>" • Payload: to = <SP-Relative-AE-ID> fr = <Registrar CSE-ID> rqi = <Request ID> rsc = <Response Status Code(2000)> pc = <Content(<CSEBase> resource representation)>
4		IOP CheckIOP Check	AE indicates successful operation
IOP Verdict			
PRO Verdict			

4.3. METODOLOGÍA DE VALIDACIÓN PARA LA UNE 178 104

Según los objetivos prácticos finales de este Estudio, y teniendo en cuenta la fase 2 del mismo, se ha considerado de especial interés el desarrollo de las especificaciones de prueba de Conformidad frente al documento UNE 178 104[12], lo que permitirá

evaluar las Plataformas de Gestión de las Ciudades Inteligentes frente al estándar nacional de referencia.

Conformidad: Implementación bajo prueba

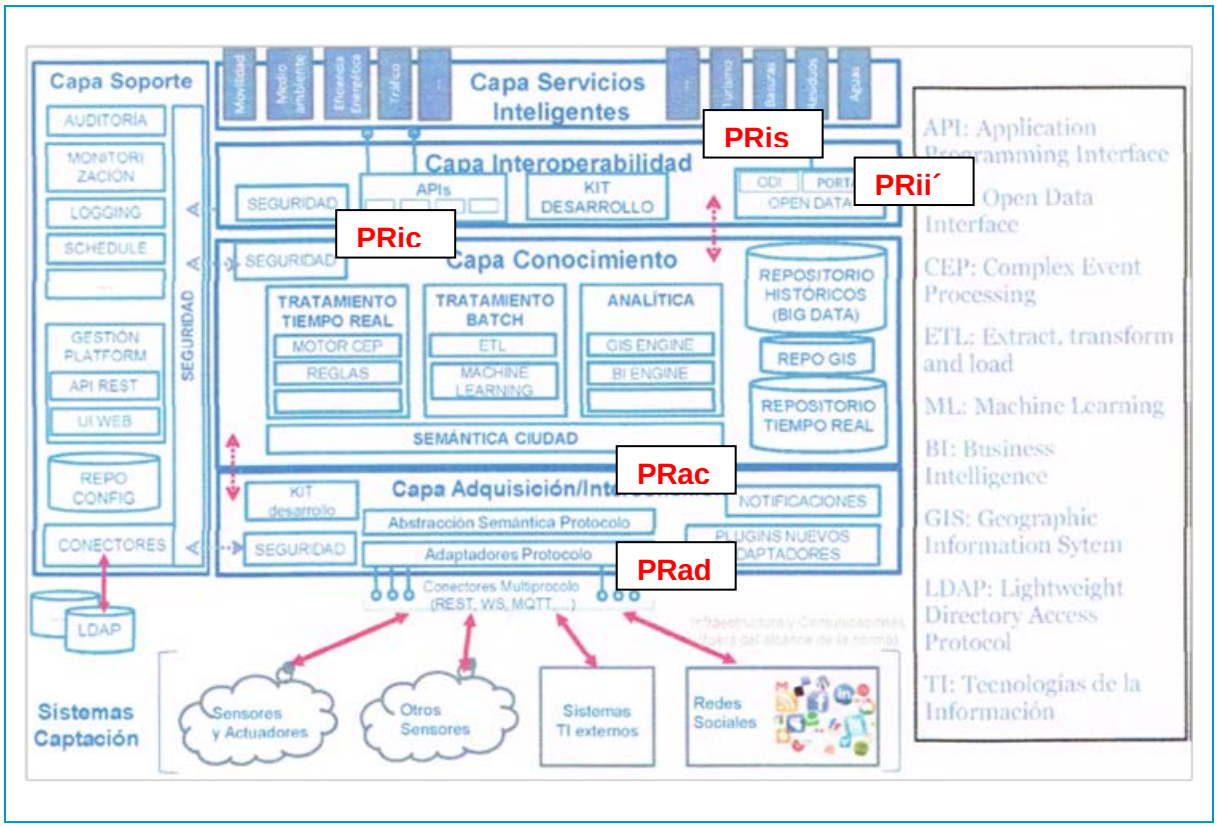
En este caso la Implementación bajo Prueba es una Plataforma de Gestión de Ciudades Inteligentes, con una arquitectura ajustada al modelo de capas propuesto en la norma:

- Sistemas de captación
- Capa de adquisición e interconexión
- Capa de conocimiento
- Capa de interoperabilidad
- Capa de servicios inteligentes

Conformidad: Puntos de referencia

Se han elegido los siguientes puntos de referencia en base a la arquitectura definida:

- **PRis**: Interfaz o punto de referencia entre la capa de Interoperabilidad y la de Servicios
- **PRic**: Interfaz o punto de referencia entre la capa de Interoperabilidad y la de Conocimiento
- **PRii´**: Interfaz o punto de referencia entre la capa de interoperabilidad de una plataforma la misma capa de otra Plataforma de un tercero
- **PRac**: Interfaz o punto de referencia entre la capa de Adquisición y la de Conocimiento
- **PRad**: Interfaz o punto de referencia entre la capa de Adquisición y los sistemas de Captación



La capa de conocimiento junto con la de soporte se consideraran como un todo (servicios comunes) de cara a su comparativa con la arquitectura oneM2M.

Conformidad: ICS

Los ICS para esta norma se basan principalmente en las métricas definidas en el mismo.

1. La arquitectura se adapta al modelo de capas especificado
    - Permite adquisición de datos desde los sistemas de captación (M)
    - Facilita la prestación de los servicios de Ciudad Inteligente (M)
    - Incluye servicios municipales y aplicaciones de negocio y valor añadido (O)
    - Ofrece servicios de soporte (M)
    - Ofrece Tratamiento, Gestión y explotación de la información (M)
2. La plataforma es modular y puede ampliar componentes, protocolos y funcionalidades (M)
3. Incorpora mecanismos de intercambio de datos con otras Plataformas (M)
4. Se basa en estándares abiertos (M)
5. Utiliza Protocolos IoT estándares (M)

6. Incorpora enfoque Big Data (M)
7. Incorpora Enfoque Opendata (M)
8. Permite Servicio en On premise (M)
9. Permite Servicio Cloud (M)
10. Tiene funciones de localización (M)
11. Incluye herramientas de uso y configuración (M)
12. Define los niveles de disponibilidad y nivel de servicio (M)
13. Dispone de Garantía, soporte y hoja de ruta (M)

M: Obligatorio

O: Opcional

Conformidad: TSS&TP

Los grupos y subgrupos se han elegido en base a la estructura del documento de referencia:

- Grupo 1: Requisitos funcionales
    - Subgrupo 1.1: Repositorio de información
    - Subgrupo 1.2: Gestión de infraestructuras
    - Subgrupo 1.3: Comunicación entre sistemas
    - Subgrupo 1.4: Seguridad
    - Subgrupo 1.5: Mantenimiento
    - Subgrupo 1.6: Desarrollo de aplicaciones
    - Subgrupo 1.7: Soporte a la decisión
    - Subgrupo 1.8: Publicación de información
    - Subgrupo 1.9: Resistencia a fallos
- Grupo 2: Requisitos técnicos
- Grupo 4: Arquitectura de capas
    - Sistemas de captación
    - Capa de adquisición e interconexión
    - Capa de conocimiento
    - Capa de interoperabilidad
    - Capa de servicios inteligentes
- Grupo 4: Interoperabilidad entre plataformas

Teniendo en cuenta los objetivos de este proyecto, en lugar de un desarrollo completo de Casos de Prueba para ser ejecutados por un laboratorio, **se va a definir un auto-cuestionario de acuerdo a lo especificado en la fase 2 de este estudio, de manera que permita identificar diferentes grados de compatibilidad** con el estándar de referencia. Este cuestionario será cumplimentado por los proveedores de Plataformas de Gestión de las Ciudades inteligentes. Las respuestas a este cuestionario serán verificables mediante aportación de las pruebas necesarias.

Los cuestionarios forman parte del documento o Parte 3: Cuestionarios [23] de este Estudio.

5. ANÁLISIS DEL GRADO DE COMPARTICIÓN POSIBLE DE APPS Y DISPOSITIVOS

A continuación se muestra el análisis de los datos suministrados por los proveedores de las Plataformas incluidas en este estudio en relación a los casos de uso seleccionados con el objetivo principal de conocer hasta qué punto es posible compartir dispositivos y gateways e incluso servicios para conseguir la interoperabilidad máxima.

Los casos de uso son los que se proponen para las Ciudades Inteligentes en el documento TR-0001 [14] de oneM2M:

- Automatización manejo de iluminación en exteriores (calles, etc.)
- Servicio de compartición de bicicletas
- Smart Parking
- Gestión Semafórica.
- Riego inteligente

Se ha elaborado un cuestionario y distribuido a diferentes suministradores de Plataformas de Ciudad Inteligente con el que se pretende analizar el cumplimiento de los estándares las facilidades que ofrecen para compartición de apps y dispositivos.

Por razones de confidencialidad, los resultados completos de los cuestionarios se encuentran en el Anexo 1 [22] a este documento o Parte 2, en un documento aparte que es considerado como confidencial y no publicable, pero las conclusiones extraídas más relevantes son:

1. Despliegue de Casos de uso: el despliegue de los casos de uso incluidos en este Estudio no se realiza de forma masiva por las Plataformas en las ciudades españolas. Algunas entidades hacen referencia a otros casos de uso si desplegados, en la mayor parte de los casos a nivel de piloto, pero no hay despliegues masivos de estos Casos de Uso tal como se plantean en el TR-0001 [16] de oneM2M para Ciudades Inteligentes.

2. Integración de casos de uso: los casos de uso implantados se integran principalmente a través de Web Services y son servicios verticales previos que se han integrado con la Plataforma para aprovechar sus capacidades y permitir la centralización de la información. También se ha detectado que en algunas de las soluciones implantadas se han desarrollado los servicios a medida para esa Plataforma.

3. Conexión directa de sensores: normalmente los sensores no se conectan directamente a las Plataformas para los casos de uso analizados, sino a través de aplicaciones previas que implementaban los casos de uso (que tenían conexión propietaria con ellos) o de gateways y concentradores que hacen de pasarela entre los sensores y la Plataforma de Gestión de ciudad inteligente. Sin embargo, todas ellas ofrecen conectores y módulos específicos para la comunicación con sensores.

4. Interfaces de comunicación. Todas ofrecen interfaces de interconexión para dispositivos y aplicaciones de terceros. A nivel físico no se detectan problemas de interoperabilidad, pero si a nivel del modelo de datos, lo que implicaría desarrollar adaptadores para la compartición de dispositivos o servicios. La publicación gratuita y abierta de los modelos de datos de cada una de las Plataformas ayudaría en gran medida a los desarrolladores a implementar las adaptaciones necesarias para cada Plataforma.

5. Facilidades de implementación e integración proporcionadas: en relación al punto anterior, todas las Plataformas ofrecen APIs, SDK y otras herramientas para facilitar la integración de dispositivos y aplicaciones de terceros.

Como conclusión final, respecto a los casos de uso seleccionados y analizados en este Estudio, no hay posibilidad directa de intercambio de sensores y servicios entre las diferentes Plataformas. Si se pueden intercambiar, realizando pequeñas adaptaciones, entre aquellas Plataformas que comparten módulos específicos del proyecto FIWARE [3] como el Context Broker o IoTAgents. Para el intercambio con otras Plataformas es necesario realizar algún otro tipo de adaptación, principalmente en el modelo de datos.

En el documento o Parte 4 de este Estudio [24] se proponen medidas específicas de fomento del grado de interoperabilidad ofrecido por los dispositivos, aplicaciones y plataformas de un ecosistema de Ciudad Inteligente.

6. ACRÓNIMOS

2G	*2nd Generation*
3G	*3rd Generation*
3GPP	*3rd Generation Partnership Project*
A2A	*Application to Application*
AAPP	*Administraciones Públicas*
AE	*Application Entity*
AEN/CTN	*Comité Técnico de Normalización de AENOR*
API	*Application Programming Interface*
APP	*Application*
ADN	*Application Dedicated Node*
ASN	*Application Service Node*
BI	*Business Intelligence*
CHA	*Continua Health Alliance*
CoAP	*Constrained Application Protocol*
CSE	*Common Service Entity*
CRUD	*Create, Retrieve, Update and Delete*
DM	*Device management*
DoS	*Denial of Service*
DUT	*Device Under Test*
ETL	*Extract, Transform and Load*
ETSI	*European Telecommunications Standards Institute*
GBA	*Generic Bootstrapping Architecture*
GIS	*Geographic Information System*
GR	*Grupo*
GSMA	*Groupe Speciale Mobile Association*
HSM	*Hardware Security Module*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
IAC	*Irrigation Administration Centre*

ICS	*Implementation Conformance Statement*
IN	*Infrastructure Node*
IoT	*Internet of Things*
IP	*Internet Protocol*
IUT	*Implementation under Test*
IXIT	*Implementation eXtra Information for Testing*
JMX	*Java Management Extensions*
JSON	*JavaScript Object Notation*
KPI	*Key Performance Indicator*
LDAP	*Lightweight Directory Access Protocol*
LWM2M	*OMA Lightweight M2M*
M	*Mandatory*
M2M	*Machine to Machine communications*
MA	*Management Adapter*
MH	*Multihop*
MN	*Middle Node*
MQTT	*Message Queue Telemetry Transport*
MS	*Management Server*
N/A	*No aplicable*
NB	*No Blocking*
NGSI	*Next Generation Service Interface*
NH	*No Hop*
NSE	*Network Service Entity*
O	*Opcional*
OMA	*Open Mobile Alliance*
PaaS	*Platform as a Service*
QoS	*Quality of Service*
REST	*Representational State Transfer*
RPO	*Recovery Point Objective*
RTO	*Recovery Time Objective*
SCADA	*Supervisory Control And Data Acquisition*

SDK	*Software Development Kit*
SGR	*Subgrupo*
SH	*Single Hop*
SLA	*Service Level Agreement*
SMS	*Short Message Service*
SNMP	*Simple Network Management Protocol*
SOAP	*Simple Object Access Protocol*
SSL	*Secure Sockets Layer*
SUT	*System Under Test*
TC	*Test Case*
TD	*Test Description*
TP	*Test Purpose*
TR	*Technical report*
TS	*Technical specification*
TLS	*Transport Layer Security*
TSS	*Test Suite Structure*
UICC	*Universal Integrated Circuit Card*
UNE	*Una Norma Española*
USIM	*Universal Subscriber Identity Module*
USSD	*Unstructured Supplementary Service Data*
VPN	*Virtual Private Network*
XML	*eXtensible Markup Language*
WAN	*Wide Area Network*

7. REFERENCIAS

[1] Interoperability best practices handbook. ETSI

[2] The interoperability enabler for the entire M2M and IOT ecosystem. White paper. oneM2M. January 2015

[3] https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/File:Fiware-citymap.jpg

[4] http://iot.tid.es/iot/thinking-city/

[5] www.sofia2.com

[6] http://web01.abertis-telecom.preproduccion.com/es/productos/smartcities/productos/

[7] https://www.carriots.com/

[8] http://www.wonderware.es/

[9] http://www-03.ibm.com/software/products/es/intelligent-operations-center

[10] http://www.redbooks.ibm.com/redbooks/pdfs/sg248061.pdf

[11] http://www.agendadigital.gob.es/planesactuaciones/Bibliotecaciudadesinteligentes/2.Materialcomplementario/normas_ciudades_inteligentes.pdf

[12] UNE 178 104 Ciudades Inteligentes (AENOR). Infraestructuras. “Sistemas integrales de gestión de la Ciudad Inteligente”

[13] UNE 178 301 (AENOR). “Ciudades Inteligentes. Datos abiertos”

[14] TS-0001 (oneM2M). “Functional Architecture”. V1.6.1

[15] TS-0002 (oneM2M). “Requirements” V1.0.1

[16] TR-0001 (oneM2M). “oneM2M Use Cases Collection” V0.0.5

[17] TS-0013 (oneM2M). “Interoperability Testing”. Borrador

[18] TS-0015 (oneM2M). “Testing Framework” Borrador

[19] TS-0017 (oneM2M). “Implementation Conformance Statement” Borrador

[20] TS-0018 (oneM2M). “Test Suite Strucutre and Test Purpose” V1.0.1

[21] Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes. Red.es. PARTE 1: Introducción.

[22] Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes. Red.es. PARTE 2: Metodología. ANEXO confidencial.

[23] Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes. Red.es. PARTE 3: Cuestionarios

[24] Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes. Red.es. PARTE 4: Soluciones Alternativas

[25] http://www.agendadigital.gob.es/planes-actuaciones/Bibliotecaciudadesinteligentes/2.Materialcomplementario/normas_ciudades_inteligentes.pdf

[26] ISO/IEC 9646 "Framework and Methodology for Conformance Testing"

Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes

PARTE 3: CUESTIONARIOS

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO
ontsi observatorio nacional de las telecomunicaciones y de la SI

Este documento constituye una aproximación parcial al estudio de la interoperabilidad en nuestras ciudades; se enmarca dentro del *Servicio para el Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes* promovido por el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información, de Red.es, y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la información.

Para la realización de este estudio se ha contado con la colaboración de AT4 wireless S.A.U.

Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes

Año 2016

ÍNDICE

1. RESUMEN EJECUTIVO

La interoperabilidad es un elemento central en el desarrollo de las Ciudades Inteligentes. El Comité Técnico de Normalización AEN/CTN 178 "Ciudades inteligentes" movilizó un amplio consenso en la redacción de la norma: "Ciudades inteligentes. Infraestructuras. Sistemas Integrales de Gestión de la Ciudad Inteligente" (UNE 178 104)[1].

El presente estudio constituye una primera aproximación al conocimiento del concepto de interoperabilidad entre plataformas de gestión de servicios inteligentes. Se trata, por tanto, de un estudio parcial ya que está centrado en estándares que no tienen exactamente el mismo objeto, puesto que la Norma UNE 178 104 es más específica para la materia que el estándar oneM2M. Desde el Plan Nacional de Ciudades Inteligentes está previsto definir estudios que aborden con mayor profundidad los casos de aplicación que se consideren relevantes.

Este documento constituye el tercero de las cuatro partes que componen el informe del estudio y recoge los cuestionarios de cumplimiento de requisitos frente a los estándares de referencia de este Estudio (UNE 178 104 [1] y TS-0001 de oneM2M [3]). Estos cuestionarios permitirán identificar los diferentes grados de compatibilidad de las Plataformas de Gestión de Ciudades Inteligentes con ambos estándares.

Se incluye una pequeña guía para cumplimentar los cuestionarios.

Así mismo se incluyen los formatos a completar por los representantes de las Plataformas de Gestión referentes a la identificación de la implementación a evaluar y de la versión del estándar, junto con las características generales y capacidades de los sistemas.

Los cuestionarios de cumplimiento para los dos estándares de referencia se presentan con las preguntas agrupadas según los grupos definidos en la metodología especificada en la primera fase de este Estudio.

Para la **UNE 178 104 [1]**:

- Grupo 1: Requisitos funcionales (RFUN)
    - Subgrupo 1.1: Repositorio de información
    - Subgrupo 1.2: Gestión de infraestructuras
    - Subgrupo 1.3: Comunicación entre sistemas
    - Subgrupo 1.4: Seguridad
    - Subgrupo 1.5: Mantenimiento
    - Subgrupo 1.6: Desarrollo de aplicaciones
    - Subgrupo 1.7: Soporte a la decisión
    - Subgrupo 1.8: Publicación de información
    - Subgrupo 1.9: Resistencia a fallos
- Grupo 2: Requisitos técnicos (RTEC)

- Grupo 3: Arquitectura de capas (ARQ)
    - Sistemas de captación
    - Capa de adquisición e interconexión
    - Capa de conocimiento
    - Capa de interoperabilidad
    - Capa de servicios inteligentes
- Grupo 4: Interoperabilidad entre plataformas (IPL)

La identificación de cada cuestión o caso de prueba es la siguiente:

TP/UNE/GR/SGR/NN

Donde UNE es el estándar de referencia, GR el grupo, SGR el subgrupo y NN un número secuencial.

Las cuestiones responden a los requisitos extraídos de la norma de referencia.

Para la TS-0001 [3], aunque para comprobar el cumplimiento del estándar será necesario, en un futuro, utilizar las especificaciones de test que está desarrollando el grupo de trabajo TST de oneM2M, en este Estudio se presenta un cuestionario que dará una estimación aproximada del cumplimiento con el estándar de referencia TS-0001 [3], basándose en el documento de requisitos TS-0002 [4] del propio oneM2M, y seleccionando solo aquellos aplicables a los nodos de infraestructura que se corresponden con el modelo de Plataformas.

También se han definido un grupo de **métricas** asociadas a cada norma, en base a las capacidades declaradas de las mismas, y a cada métrica se han asociado un conjunto de cuestiones relacionadas. Así mismo, hay cuestiones que se considera que pueden tener un impacto mayor o menor en la adecuación de las Plataformas con los objetivos que se persiguen en este estudio. Por esta razón, el peso de cada cuestión es diferente.

Para el cálculo del valor final asociado a cada una de las métricas, se considerarán aquellas cuestiones a las que se ha respondido afirmativamente y se ha justificado dicha respuesta (en caso contrario será 0). El valor final se calcula realizando la suma de todos los porcentajes de las preguntas consideradas como positivas.

2. OBJETIVOS DEL DOCUMENTO

El objetivo final es buscar la portabilidad y reutilización de las aplicaciones y la compartición de dispositivos sobre las diferentes Plataformas de Gestión de Ciudades Inteligentes. Este estudio constituye una primera aproximación al conocimiento del concepto de interoperabilidad entre plataformas de gestión de servicios inteligentes. Desde el Plan Nacional de Ciudades Inteligentes está previsto definir estudios que aborden con mayor profundidad los casos de aplicación que se consideren relevantes.

Además se pretende conocer el posible impacto de la estandarización que se está llevando a cabo tanto a nivel nacional, en el CTN 178 de AENOR, como internacional, en el oneM2M, y sus posibles consecuencias en el desarrollo de soluciones Smart Cities en España, y tomar, a partir de las conclusiones de este Estudio, las medidas que se consideren oportunas.

Para ello, el Estudio se ha dividido en las siguientes fases:

- **E1: FASE 1**

  1. **Identificación de puntos de referencia (o confluencia de estándares)** entre los que se puede establecer comparativa entre el modelo de capas propuesto en el documento UNE 178 104 [1] de AENOR y la arquitectura oneM2M [3].

  2. Definición de una **metodología de análisis y cumplimiento de requisitos** para diferentes plataformas comerciales y casos de uso frente a los estándares de referencia.

  3. **Analizar Casos de Uso** reales implantados en diferentes ciudades nacionales conforme establece oneM2M [5]. Los Casos de Uso seleccionados son:

     - Automatización manejo de iluminación en exteriores (calles, etc.)
     - Servicio de compartición de bicicletas
     - Smart Parking
     - Gestión Semafórica
     - Riego inteligente

- **E2: FASE 2**

  Elaboración de **cuestionarios** de cumplimiento de requisitos frente a los estándares de referencia que permitan identificar diferentes grados de compatibilidad con los mismos.

- **E3: FASE 3**

  Propuesta de **soluciones interinas** que pudieran ser utilizadas para asegurar la interoperabilidad de las plataformas seleccionadas, en los casos de uso anteriores, minimizando en lo posible los costes de desarrollo, pero siempre admitiendo, a medio plazo, una evolución hacia los estándares propuestos en oneM2M.

Para completar este Estudio se han generado cuatro documentos, uno introductorio y otros tres correspondientes a cada una de las Fases definidas. El presente documento constituye el resultado de la Fase 2 del Estudio.

El objetivo de este documento es definir cuestionarios para que los proveedores de Plataformas puedan realizar una autoevaluación de sus sistemas frente a los estándares de referencia [1][3].

En ningún caso forma parte de este estudio la evaluación en sí de las Plataformas frente a estos estándares, sino el desarrollo de las herramientas necesarias para la autoevaluación, a lo largo del tiempo, de las Plataformas de Gestión de Ciudades Inteligentes, detectando los puntos de mejora de las mismas desde el punto de vista de cumplimiento de estándares y así poder definir la hoja de ruta de desarrollo persiguiendo el objetivo del cumplimiento de los estándares de referencia.

3. FASE 2: CUESTIONARIOS

Este cuestionario de cumplimiento de requisitos tiene como objetivo identificar los grados de compatibilidad de las Plataformas de Gestión, en un instante determinado, frente a estándares de referencia. Podrá ser utilizado por los proveedores de Plataformas para realizar una evaluación de sus sistemas frente a los estándares UNE 178 104 [1] y oneM2M TS-0001 V1.6.1 [3].

Los cuestionarios tienen la siguiente estructura:

- Guía para cumplimentarlo
- Identificación de la implementación a evaluar
- Identificación de la versión del estándar
- Características generales y capacidades
- Cuestiones
- Métricas aplicables

Donde los tres primeros puntos son comunes para ambos estándares, mientras que el resto está particularizado para cada uno de ellos.

3.1. GUÍA PARA CUMPLIMENTARLO

Para cumplimentar los apartados siguientes y posteriormente calcular el porcentaje de cumplimiento de la Plataforma de Gestión frente a los estándares de referencia siga los siguientes pasos:

NOTA: Se recomienda que la persona que complete los cuestionarios y el que realice la asignación de puntuación para las métricas sean diferentes.

1. Identifique la implementación a evaluar completando la tabla del apartado 3.2 de este documento.
2. Identifique el estándar frente al que evaluar la implementación: TS-0001 o UNE 178 104 (apartado 3.3).
3. Indique, seleccionando Si/No, los puntos de referencia y capacidades que incorpora la implementación a evaluar:
    a. Completando el apartado 3.4.1 para el estándar UNE 178 104
    b. Completando el apartado 3.4.2 para el estándar TS-0001
4. Complete los cuestionarios correspondientes contestando a la pregunta realizada con Si/No y desarrolle la respuesta en caso de que así se indique. Añada las observaciones que crea oportunas en el apartado de otras observaciones.
5. Una vez completados los cuestionarios, realice la asignación de puntuaciones como se describe en el apartado 3.6 y aplique el peso definido para cada una de las puntuaciones. Sume los porcentajes obtenidos para cada métrica y se obtendrá el porcentaje de cumplimiento de la métrica en cuestión, lo que indicará el grado de cumplimiento respecto del estándar de referencia.

3.2. IDENTIFICACIÓN DE LA IMPLEMENTACIÓN A EVALUAR

Item	Descripción	Notas
Identificación del proveedor		
Proveedor		
Dirección		
Ciudad		
País		
Nombre Persona de contacto		
Teléfono Persona de contacto		
e-mail Persona de contacto		
Otros contactos		
Nombre del evaluador		
Fecha de realización de la validación	Fecha de inicio: Fecha de final:	
Identificación de la Plataforma		
Modelo		Si está formado por diferentes módulos incluirlos todos
Descripción de la configuración hardware requerida		
Sistema operativo		
Descripción de la configuración software requerida		

3.3. IDENTIFICACIÓN DE LA VERSIÓN DEL ESTÁNDAR

Habrá que seleccionar entre los estándares de referencia:

- UNE 178 104
- oneM2M TS-0001 V1.6.1

3.4. CARACTERÍSTICAS GENERALES Y CAPACIDADES

3.4.1. UNE 178 104

Para la evaluación frente al UNE 178 104 [1], indique si están incluidos o no los siguientes puntos de referencia o capacidades:

Puntos de referencia

PUNTO DE REFERENCIA	SOPORTADO
PRis	Si [ ] No [ ]
PRic	Si [ ] No [ ]
PRii´	Si [ ] No [ ]
PRac	Si [ ] No [ ]
PRad	Si [ ] No [ ]

Donde:

- **PRis**: Interfaz o punto de referencia entre la capa de Interoperabilidad y la de Servicios
- **PRic**: Interfaz o punto de referencia entre la capa de Interoperabilidad y la de Conocimiento
- **PRii´**: Interfaz o punto de referencia entre la capa de interoperabilidad de una plataforma la misma capa de otra Plataforma de un tercero
- **PRac**: Interfaz o punto de referencia entre la capa de Adquisición y la de Conocimiento
- **PRad**: Interfaz o punto de referencia entre la capa de Adquisición y los sistemas de Captación

Nota: La definición de los puntos de referencia está incluida en el documento o Parte 2 de este Estudio.

Capacidades

CAPACIDAD	SOPORTADO
1. La arquitectura se adapta al modelo de capas especificado	Si [ ] No [ ]
2. Permite adquisición de datos desde los sistemas de captación	Si [ ] No [ ]
3. Facilita la prestación de los servicios de Ciudad Inteligente	Si [ ] No [ ]
4. Incluye servicios municipales y aplicaciones de negocio y valor añadido	Si [ ] No [ ]
5. Ofrece servicios de soporte	Si [ ] No [ ]
6. Ofrece Tratamiento, Gestión y explotación de la información	Si [ ] No [ ]
7. La plataforma es modular y puede ampliar componentes, protocolos y funcionalidades	Si [ ] No [ ]
8. Incorpora mecanismos de intercambio de datos con otras Plataformas	Si [ ] No [ ]
9. Se basa en estándares abiertos	Si [ ] No [ ]
10. Utiliza Protocolos IoT estándares	Si [ ] No [ ]
11. Incorpora enfoque Big Data	Si [ ] No [ ]
12. Incorpora Enfoque Opendata	Si [ ] No [ ]

13. Permite Servicio en On premise	Si [ ] No [ ]
14. Permite Servicio Cloud	Si [ ] No [ ]
15. Tiene funciones de localización	Si [ ] No [ ]
16. Incluye herramientas de uso y configuración	Si [ ] No [ ]
17. Define los niveles de disponibilidad y nivel de servicio	Si [ ] No [ ]
18. Dispone de Garantía, soporte y hoja de ruta	Si [ ] No [ ]

3.4.2. TS-0001

Puntos de referencia

PUNTO DE REFERENCIA	SOPORTADO
Mca	Si [ ] No [ ]
Mcc	Si [ ] No [ ]
Mcn	Si [ ] No [ ]
Mcc´	Si [ ] No [ ]

Nota: Estos puntos de referencia son los definidos en el estándar oneM2M TS-0001 [3].

Capacidades

CAPACIDAD	SOPORTADO
1. Registro	Si [ ] No [ ]
2. Gestión de datos	Si [ ] No [ ]
3. Suscripción y notificación	Si [ ] No [ ]
4. Gestión de grupos	Si [ ] No [ ]
5. Descubrimiento	Si [ ] No [ ]
6. Gestión de la localización	Si [ ] No [ ]
7. Gestión de dispositivos	Si [ ] No [ ]
8. Gestión de las comunicaciones y de entregas	Si [ ] No [ ]

3.5. CUESTIONES

3.5.1. UNE 178 104

Para la identificación de las cuestiones, se va a utilizar la clasificación realizada en el apartado TSS&TP de definición de la metodología, recogida en el documento o Parte número 2 de este Estudio [7], que es la siguiente:

- Grupo 1: Requisitos funcionales (RFUN)
    - Subgrupo 1.1: Repositorio de información (REP)
    - Subgrupo 1.2: Gestión de infraestructuras (INFR)
    - Subgrupo 1.3: Comunicación entre sistemas (INT)

- Subgrupo 1.4: Seguridad (SEC)
- Subgrupo 1.5: Mantenimiento (MANT)
- Subgrupo 1.6: Desarrollo de aplicaciones (APP)
- Subgrupo 1.7: Soporte a la decisión (DSS)
- Subgrupo 1.8: Publicación de información (PUBL)
- Subgrupo 1.9: Resistencia a fallos (FALL)

- Grupo 2: Requisitos técnicos (RTEC)
- Grupo 3: Arquitectura de capas (ARQ)
  - Capa de adquisición e interconexión (ADQ)
  - Capa de conocimiento (CON)
  - Capa de interoperabilidad (INT)
  - Capa de servicios inteligentes (SER)
  - Capa de soporte (SOP)
- Grupo 4: Interoperabilidad entre plataformas (IPL)

La identificación de cada cuestión o caso de prueba es la siguiente:

TP/UNE/GR/SGR/NN

Donde UNE es el estándar de referencia, GR el grupo, SGR el subgrupo y NN un número secuencial.

Las cuestiones responden a los requisitos extraídos de la norma de referencia y recogidos en el segundo documento o Parte 2 de este Estudio.

REQUISITOS FUNCIONALES. REPOSITORIO DE INFORMACIÓN

ID	DESCRIPCIÓN
TP/UNE/RFUN/REP/01	¿Contiene un catálogo común, universal, mantenido, accesible y clasificado de datos únicos y normalizados de la ciudad? ¿En qué módulo funcional?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/REP/02	¿Posee un catálogo de activos? ¿Qué nomenclatura utiliza para los activos?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/REP/03	¿Permite visiones analíticas transversales de la ciudad a partir de estos datos? ¿En qué módulo funcional?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/REP/04	¿Integra datos y legacy de otras soluciones existentes en la ciudad? ¿Cuáles?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/REP/05	¿La plataforma explota los datos y permite a otras apps hacerlo? ¿En qué módulos funcionales?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

REQUISITOS FUNCIONALES. GESTIÓN DE INFRAESTRUCTURAS

ID	DESCRIPCIÓN
TP/UNE/RFUN/INFR/01	¿Soporta acceso a los datos de plataformas de sensores, bases de datos y a información de otras aplicaciones? ¿Qué interfaces ofrece para ello?
Si [ ] No [ ] Respuesta:	

Otras observaciones:

ID	DESCRIPCIÓN
TP/UNE/RFUN/INFR/02	¿Permite actuaciones sobre actuadores (sensores) a través de soluciones estandarizadas? ¿Qué soluciones?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/INFR/03	¿Se realiza un registro de las actividades que se desarrollan en el sistema? ¿Qué tipo de actividades registra?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/INFR/04	¿Gestiona el mantenimiento de equipos e infraestructuras? ¿En qué módulo funcional?
Si [ ] No [ ] Respuesta:	

Otras observaciones:

ID	DESCRIPCIÓN
TP/UNE/RFUN/INFR/05	¿Soporta los protocolos para monitorización SNMP y JMX?
Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/INFR/06	¿Permite la integración con otros sistemas y aplicaciones de terceros? ¿A través de que interfaz?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

REQUISITOS FUNCIONALES. COMUNICACIÓN ENTRE SISTEMAS (INTEROPERABILIDAD)

ID	DESCRIPCIÓN
TP/UNE/RFUN/INT/01	¿Provee las interfaces necesarias para que eventos de un sistema puedan desencadenar acciones en otros? ¿Cuáles son las interfaces?
Si [ ] No [ ] Respuesta	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/INT/02	¿Tiene APIs y protocolos normalizados para comunicación con otras aplicaciones? ¿Cuáles son?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/INT/03	¿Permite incluir nuevos protocolos de comunicación con sensores? ¿Cómo?
Si [ ] No [ ] Respuesta:	

Otras observaciones:

REQUISITOS FUNCIONALES. SEGURIDAD

ID	DESCRIPCIÓN
TP/UNE/RFUN/SEC/01	¿Soporta autenticación y autorización? ¿En qué modulo funcional?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/SEC/02	¿Realiza control de acceso a todos los elementos a los que se accede a través de la plataforma? ¿Donde se gestionan los permisos?
Si [ ] No [ ] Parcialmente [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/SEC/03	¿Se garantiza la confidencialidad en las comunicaciones? ¿Cómo?
Si [ ] No [ ]	

Respuesta:
Otras observaciones:

ID	DESCRIPCIÓN
TP/UNE/RFUN/SEC/04	¿Se garantiza la confidencialidad en el acceso a los datos, de modo que cada rol sólo pueda ver los datos a los que tiene acceso? ¿Qué roles se definen?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/SEC/05	¿Define y gestiona políticas de seguridad? ¿En qué modulo funcional?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/SEC/06	¿Provee una interfaz vía web para poder realizar gestiones de administración de los usuarios, roles y permisos? ¿Cuál es?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/SEC/07	¿Soporta mecanismos de autenticación como soluciones basadas en usuario y contraseña en tokens, en OAuth, en certificados electrónicos (de individuos, servidores y aplicaciones) u otro tipo de soluciones avanzadas basadas, por ejemplo, en técnicas biométricas? ¿Cuáles soporta?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/SEC/08	¿Permite la integración con otros repositorios de usuarios ya existentes como LDAP, bases de datos, etc.? ¿Cuáles soporta?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/SEC/09	¿Tiene capacidad de adaptar los mecanismos de seguridad a las necesidades propias de cada ciudad? ¿En qué modulo funcional?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/SEC/10	¿Asegura la privacidad y seguridad de los datos almacenados? ¿Cómo?
Si [ ] No [ ] Respuesta:	

Otras observaciones:

ID	DESCRIPCIÓN
TP/UNE/RFUN/SEC/11	¿Garantiza el envío/recepción segura de datos desde/hacia los dispositivos conectados al sistema, así como su distribución segura a los aplicativos que los requieran? ¿Cómo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/SEC/12	¿La gestión de roles/permisos contempla al menos los siguientes niveles de seguridad? • Acceso a los datos: limitar la información que puede visualizar cada usuario. • Acceso a los elementos de la Plataforma Integral: limitar el acceso a los informes y cuadro de mando configurados en la Plataforma Integral • Funcionalidad: delimitar las acciones que puede realizar un determinado usuario en función de su perfil ¿En qué modulo funcional?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

REQUISITOS FUNCIONALES. MANTENIMIENTO

ID	DESCRIPCIÓN
TP/UNE/RFUN/MANT/01	¿Almacena y hace valoración de indicadores relevantes para la gestión del mantenimiento? ¿Qué indicadores?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/MANT/02	¿Genera planes de mantenimiento a partir de indicadores relevantes para la gestión del mantenimiento? ¿Periódicamente o bajo petición?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/MANT/03	¿Gestiona los avisos o alarmas y puede enviar mensajes, correos, SMS y llamadas en función de indicadores relevantes para la gestión del mantenimiento? ¿Qué métodos se usan para los avisos?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/MANT/03	¿Permite integración nativa con sistemas móviles y APPs? ¿A través de que modulo funcional?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

REQUISITOS FUNCIONALES. DESARROLLO DE APLICACIONES

ID	DESCRIPCIÓN
TP/UNE/RFUN/APP/01	¿Permite realizar análisis de consumos, alarmas, tendencias, etc? ¿Dónde se publican y almacenan?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/APP/02	¿Permite imputación de costes? ¿En qué modulo funcional?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/APP/03	¿Permite optimización de procesos y planificación? ¿En qué modulo funcional?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/APP/04	¿Permite realizar un control de calidad de servicios públicos de terceros? ¿En qué modulo funcional?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/APP/05	¿Contempla una sala de crisis? ¿Cómo se accede?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/APP/06	¿Soporta informes de explotación? ¿Periódicos o bajo demanda?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/APP/07	¿Se integra con otras herramientas para el análisis de indicadores? ¿Con cuales?
Si [ ] No [ ] Respuesta:	

Otras observaciones:

REQUISITOS FUNCIONALES. SOPORTE A LA DECISIÓN

ID	DESCRIPCIÓN
TP/UNE/RFUN/DSS/01	¿Integra herramientas de simulación en base a la información actual e histórica? ¿Cuáles?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/DSS/02	¿Integra herramientas de valoración y ejecución de planes de actuación, en escenarios complejos? ¿Cuáles?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/DSS/03	¿Integra herramientas de análisis predictivo y modelado de la ciudad? ¿Cuáles?
Si [ ] No [ ] Respuesta:	

Otras observaciones:

ID	DESCRIPCIÓN
TP/UNE/RFUN/DSS/04	¿Integra herramientas de minería de datos y el análisis estadístico? ¿Cuáles?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/DSS/05	¿Dispone de herramientas de integración con otros sistemas y herramientas de Business Inteligence? ¿Cuáles?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

REQUISITOS FUNCIONALES. PUBLICACIÓN DE INFORMACIÓN

ID	DESCRIPCIÓN
TP/UNE/RFUN/PUBL/01	¿Transmite información abierta y en formatos estándar? ¿Qué información?
Si [ ]	No [ ]

Respuesta:
Otras observaciones:

ID	DESCRIPCIÓN
TP/UNE/RFUN/PUBL/02	¿La información publicada es accesible desde multidispositivos? ¿Desde cuáles?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/PUBL/03	¿Permite transmitir la información de forma continua y sin interrupciones?
Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/PUBL/04	¿Transmite información aplicable a servicios finales al ciudadano (sociedad de la información)? ¿A cuáles?
Si [ ] No [ ] Respuesta:	

Otras observaciones:

ID	DESCRIPCIÓN
TP/UNE/RFUN/PUBL/05	¿Transmite información aplicable a servicios aplicaciones de terceros? ¿Qué información?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/PUBL/06	¿Transmite información aplicable a otros servicios públicos y administraciones? ¿Qué información?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/PUBL/07	¿Transmite información aplicable a rendición de cuentas (transparencia)? ¿Qué información?
Si [ ] No [ ] Respuesta:	

Otras observaciones:

REQUISITOS FUNCIONALES. RESISTENCIA A FALLOS

ID	DESCRIPCIÓN
TP/UNE/RFUN/FALL/01	¿Se garantiza la continuidad operativa de los servicios inteligentes de acuerdo con los niveles de servicios contratados? ¿Cuál es el SLA tipo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RFUN/FALL/02	¿Se garantiza la recuperación en caso de desastres como un RTO (Objetivo de Tiempo de Recuperación) y un RPO (Objetivo de Punto de Recuperación) limitados? ¿Cuáles son como mínimo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

REQUISITOS TÉCNICOS

ID	DESCRIPCIÓN
TP/UNE/RTEC/01	¿Es una plataforma horizontal que soporta diferentes casos de uso? Ponga algunos ejemplos.
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RTEC/02	¿Tiene capacidad de soporte de diferentes tecnologías, dispositivos y mecanismos de captura de información, y estándares de comunicación, así como otros sistemas de información internos/corporativos y/o externos?
Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RTEC/03	¿Posee la habilidad para manejar en tiempo real un elevado número de dispositivos, servicios y procesos de manera eficiente? Indique el número máximo de dispositivos que puede manejar.
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RTEC/04	¿Permite poder incrementar capacidad de proceso y almacenamiento sin tener que modificar la arquitectura? ¿Cómo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RTEC/05	Robustez y Resiliencia: ¿Tiene la capacidad para seguir funcionando ante problemas? Describir los métodos que aplica
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RTEC/06	¿Tiene un enfoque modular que permite desplegarla por partes de forma sencilla? Describir algún ejemplo
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RTEC/07	Continuidad operativa o disponibilidad: ¿tiene la capacidad para estar operativo en cualquier momento? ¿Qué mecanismos implementa?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RTEC/08	¿Tiene la capacidad para gestionar de forma eficiente los fallos que puedan afectar a la disponibilidad? ¿Qué mecanismos implementa?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RTEC/09	Flexibilidad: ¿Tiene la habilidad para funcionar con diferentes servicios inteligentes de ciudad? Poner algunos ejemplos.
Si [ ] No [ ] Respuesta:	

Otras observaciones:

ID	DESCRIPCIÓN
TP/UNE/RTEC/10	Extensibilidad: ¿tiene la capacidad para poder ampliarse para dar soporte a nuevas necesidades? Poner algunos ejemplos (aumento de almacenamiento, nuevos sensores, nuevas APIs, etc…).
Si [ ] Respuesta:	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RTEC/11	¿Tiene capacidades Big Data? ¿En qué modulo funcional?
Si [ ] Respuesta:	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RTEC/12	¿Está basada en estándares abiertos para integración? ¿Cuáles?
Si [ ]	No [ ]

Respuesta:
Otras observaciones:

ID	DESCRIPCIÓN
TP/UNE/RTEC/13	¿Tiene capacidad de extensión en el futuro mediante estándares ampliamente adoptados? ¿Cómo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RTEC/14	¿Es una plataforma integral o formada por piezas desacopladas? Describir
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RTEC/15	Operable y gestionable: ¿se gestiona, opera, mantiene y se instala de forma sencilla? Indicar los perfiles

	requeridos para operar, gestionar, mantener e instalar la plataforma.
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RTEC/16	¿Utiliza conceptos semánticos estándares si existe disponibilidad? ¿En qué estándares se basa?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/RTEC/17	¿Se garantiza la seguridad, privacidad y confianza? Detallar algunos mecanismos
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ARQUITECTURA DE CAPAS

ID	DESCRIPCIÓN
TP/UNE/ARQ/01	¿La plataforma se ajusta al sistema de capas propuesto en el documento?
Si [ ]	No [ ]
Otras observaciones:	

ARQUITECTURA DE CAPAS. CAPA DE ADQUISICIÓN/INTERCONEXIÓN

ID	DESCRIPCIÓN
TP/UNE/ARQ/ADQ/01	¿Es independiente del operador de red?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/ARQ/ADQ/02	¿Permite integración de la información desde las fuentes de datos (sensores, dispositivos etc…)? ¿Qué conectores implementa?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/ARQ/ADQ/03	¿Suministra información a la capa de conocimiento con independencia de los dispositivos dando una vista semántica de los datos adquiridos? ¿Qué semántica implementa?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/ARQ/ADQ/04	¿Tiene interfaces abiertos y estandarizados sobre los que es posible desarrollar aplicaciones de terceros que interactúen directamente con los dispositivos, no propietarios? ¿Qué interfaces implementa?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/ARQ/ADQ/05	¿Tiene una única capa de adquisición para todos los servicios?
Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/ARQ/ADQ/06	¿Es independiente de la tecnología de acceso y los sensores?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/ARQ/ADQ/07	¿Es posible añadir nuevos conectores? ¿Cómo?
Si [ ] Respuesta:	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/ARQ/ADQ/08	¿Permite acceder a los datos, control y configuración de los sensores?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/ARQ/ADQ/09	¿Tiene un modulo capaz de conectar escenarios compatibles con oneM2M? ¿Cuál?
Si [ ] Respuesta:	No [ ]

Otras observaciones:

ARQUITECTURA DE CAPAS. CAPA DE CONOCIMIENTO

ID	DESCRIPCIÓN
TP/UNE/ARQ/CON/01	¿Permite acceso a la información histórica y en tiempo real? ¿Cómo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/ARQ/CON/02	¿Recibe datos de la capa de adquisición para almacenamiento, proceso y recuperación y los pone a disposición de la capa de interoperabilidad siguiendo modelos de datos? ¿Qué datos ofrece a la capa de interoperabilidad?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN

TP/UNE/ARQ/CON/03	¿Soporta tratamiento en tiempo real de los datos recibidos de la capa de adquisición a través de motor de reglas?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/ARQ/CON/04	¿Soporta tratamiento Batch de los datos recibidos a través de ETL?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/ARQ/CON/05	¿Soporta tratamiento analítico de los datos mediante proceso BI (Business Intelligence)?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/ARQ/CON/06	¿Soporta tratamiento GIS, permitiendo georeferencias de datos y hacer consultas geográficas?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/ARQ/CON/07	¿Se controla el acceso mediante usuario/rol de cada tipo de datos?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/ARQ/CON/08	¿Aplica semánticas creadas por organizaciones internacionales o las crea, si no existen vocabularios, y las publica? Citar las creadas por las organizaciones y las publicadas
Si [ ] Respuesta:	No [ ]
Otras observaciones:	

ARQUITECTURA DE CAPAS. CAPA DE INTEROPERABILIDAD

ID	DESCRIPCIÓN
TP/UNE/ARQ/CINT/01	¿Publica APIs tipo REST con diferentes modos de acceso (Incluyendo modo Push y Pull) así como consultas georeferenciadas? ¿Cuáles?
Si [ ] Respuesta:	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/ARQ/CINT/02	¿Tiene una interfaz para interconexión con otras plataformas y aplicaciones? ¿Cuál?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/ARQ/CINT/03	¿Permite acceso a servicios externos? Cite algunos
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/ARQ/CINT/04	¿Tiene un portal opendata? ¿Cómo se accede?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN

TP/UNE/ARQ/CINT/05	¿Tiene kit de desarrollo con SDK y APIs para construir servicios? ¿Cuáles?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/ARQ/CINT/06	¿Usa un modelo de acceso a datos según oneM2M? ¿Cuál es el modelo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ARQUITECTURA DE CAPAS. CAPA DE SERVICIOS INTELIGENTES

ID	DESCRIPCIÓN
TP/UNE/ARQ/SER/01	¿Tiene un centro de mandos personalizados e indicadores para diferentes ubicaciones de despliegue en función del perfil y de los permisos del usuario? ¿En qué módulo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/ARQ/SER/02	¿Tiene aplicaciones de gestión de servicios verticales? ¿Cuáles?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/ARQ/SER/03	¿Realiza gestión de contratos y tiene SLA en bases de datos?
Si [ ] No [ ]	
Otras observaciones:	

ARQUITECTURA DE CAPAS. CAPA DE SOPORTE

ID	DESCRIPCIÓN
TP/UNE/ARQ/SOP/01	¿Tiene un entorno Web de Gestión de la configuración, incluyendo interfaces REST de gestión? ¿En qué módulo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/ARQ/SOP/02	¿Tiene un repositorio de almacenamiento de la configuración centralizado? ¿En qué módulo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/ARQ/SOP/03	¿Provee seguridad de acceso y Conectores de Repositorio de Seguridad? ¿Cómo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

INTEROPERABILIDAD ENTRE PLATAFORMAS

ID	DESCRIPCIÓN
TP/UNE/IPL/01	¿Tiene Independencia en el dominio de las APPs?
Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/IPL/02	¿Tiene Independencia en el dominio de la red?

Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/UNE/IPL/03	¿Tiene Independencia en el dominio de la adquisición de datos?
Si [ ] No [ ]	
Otras observaciones:	

3.5.2. TS-0001

Para la TS-0001 [3], aunque para comprobar el cumplimiento del estándar será necesario, en un futuro, utilizar las especificaciones de test que está desarrollando el grupo de trabajo TST de oneM2M, en este Estudio se presenta un cuestionario que dará una estimación aproximada del cumplimiento con el estándar de referencia TS-0001 [3], basándose en el documento de requisitos TS-0002 [4] del propio oneM2M, y seleccionando solo aquellos aplicables a los nodos de infraestructura que se corresponden con el modelo de Plataformas.

La identificación de las cuestiones será la siguiente:

TP/M2M/GR/SGR/NN

Donde M2M es el estándar de referencia, GR el grupo, SGR el subgrupo (si aplica) y NN un número secuencial. Los grupos son los definidos en el documento oneM2M TS-0002 “Requirements” [4].

- Grupo 1: Requisitos generales (OSR)
- Grupo 2: Requisitos de gestión (MGR)
- Grupo 3: Requisitos de gestión (MGR)
- Grupo 4: Requisitos de abstracción (ABR)
- Grupo 5: Requisitos semánticos (SMR)
- Grupo 6: Requisitos de seguridad (SER)
- Grupo 7: Requisitos de tarificación (CHG)

- Grupo 8: Requisitos operacionales (OPR)
- Grupo 9: Requisitos de gestión de la comunicación (CMR)

REQUISITOS GENERALES

ID	DESCRIPCIÓN
TP/M2M/OSR/01	¿Permite comunicación entre aplicaciones usando múltiples medios de comunicación basados en IP? ¿A través de qué interfaces?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/02a	¿Permite comunicación con dispositivos con computación reducida (ej. pequeña CPU, memoria, batería, etc.) o capacidades de comunicación reducidas (ej. modem 2G)? ¿A través de qué interfaces?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/02b	¿Permite comunicación con dispositivos con gran capacidad de computación (ej. gran CPU, memoria, batería, etc.) o capacidades de comunicación reducidas (ej. modem 3G)? ¿A través de qué interfaces?

Si [ ] No [ ] Respuesta:
Otras observaciones:

ID	DESCRIPCIÓN
TP/M2M/OSR/03	¿Soporta comunicaciones entre aplicaciones con establecimiento de sesión?
Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/04	¿Soporta comunicaciones entre aplicaciones sin inicio de sesión?
Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/05	¿Descubre servicios proporcionados por redes de comunicación a aplicaciones M2M (ej. SMS, USSD, localización, configuración de suscripción, autenticación, etc.) sujetos a las reglas de restricción del operador de red?
Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/06	¿Reutiliza servicios ofrecidos por las redes subyacentes a través de modelos de acceso abiertos (ej. OMA, framework GSMA OneAPI). Algunos ejemplos de servicios son: • Comunicaciones IP multimedia. • Mensajería • Localización. • Servicios de facturación. • Información de dispositivos y perfiles. • Configuración y gestión de dispositivos. • Activación y monitorización de dispositivos. • Pequeñas transmisiones de datos. • Gestión de grupos ¿Cuáles en concreto?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/07	¿Provee un mecanismo para que las aplicaciones M2M interactúen con otras y con los datos/información de proveedores de servicio M2M diferentes con los permisos apropiados? ¿Puede describir el flujo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN

TP/M2M/OSR/08	¿Provee la capacidad para que aplicaciones M2M se comuniquen con dispositivos M2M sin la necesidad de conocer la tecnología y el protocolo de comunicación específico del dispositivo M2M? Cite un ejemplo.
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/09	¿Soporta la capacidad de que una o múltiples aplicaciones M2M interactúen con uno o múltiples gateways/dispositivos M2M? ¿A través de qué interfaz?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/10	¿Soporta mecanismos de envío de mensajes con confirmación a otras aplicaciones y detecta fallos de envío en un intervalo de tiempo dado?
Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/11a	¿Tiene la capacidad de solicitar diferentes caminos de comunicación con mecanismos de enrutamiento para evitar fallos en la transmisión? ¿En qué módulo se realiza?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/11b	¿Tiene la capacidad de solicitar diferentes caminos de comunicación según las peticiones de aplicaciones M2M?
Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/12	¿Soporta comunicaciones entre aplicaciones M2M y dispositivos soportando servicios M2M por medio de una conectividad continua o no-continua? ¿A través de qué interfaz?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/13	¿Conoce la tolerancia de retardo aceptable por la aplicación M2M y lo indica a la red subyacente?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/14	¿Puede comunicarse con dispositivos M2M, detrás de un Gateway M2M que soporta heterogéneas redes M2M? Ponga un ejemplo
Si [ ] Respuesta:	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/15	¿Soporta diferentes patrones de comunicación incluyendo comunicaciones poco frecuentes, transferencia de pequeñas cantidades de datos, transferencia de grandes archivos y comunicaciones en streaming? Cite los que soporta
Si [ ] Respuesta:	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/16	¿Provee la capacidad de notificar a aplicaciones M2M sobre la disponibilidad, cambios de aplicaciones o información de gestión de un dispositivo/gateway M2M, incluyendo cambios en la red M2M? ¿En qué módulo se realiza?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/17	¿Ofrece a los servicios de terceros los siguientes servicios: • Gestión de la conectividad. • Gestión de dispositivos. • Gestión de datos de aplicación. Cite cuales y desde que modulo se gestionan
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/18	¿Ofrece servicios M2M a dispositivos en itinerancia a través las redes subyacentes celulares, según las restricciones basadas en las reglas del operador de red? ¿A qué dispositivos? Ponga un ejemplo.
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/19	¿Soporta la capacidad de repositorio de datos y de transferencia de datos entre dispositivos/gateways M2M, infraestructuras de servicios M2M o infraestructuras de aplicaciones M2M, de la siguiente manera: • Acción iniciada por un dispositivo o gateway M2M, infraestructuras de servicios M2M o infraestructuras de aplicaciones M2M. • Iniciada por un evento o una activación programada. • Por datos específicos Cite cuales
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/20	¿Admite y gestiona reglas sobre los aspectos de almacenamiento y recuperación de datos/información? ¿En qué módulo/s?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/21	¿Provee mecanismos para permitir compartir datos entre múltiples aplicaciones M2M? ¿Cuáles?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/22	¿Provee mecanismos para garantizar la disponibilidad en caso de fallo de algún elemento? ¿Cuáles?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/23	¿Identifica los servicios M2M que pone a disposición de otros servicios suscriptores? ¿Cómo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/24	¿Identifica a los dispositivos que pone a disposición de los servicios subscriptores? ¿Cómo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/25	¿Identifica a las aplicaciones que pone a disposición de los servicios subscriptores? ¿Cómo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/26	¿Puede asociar dispositivos M2M con los identificadores de dispositivo ofrecidos por la red subyacente y/o el dispositivo? ¿Cómo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/27	¿Provee un mecanismo para permitir intercambio de datos de forma transparente entre una aplicación M2M y la red?
Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/28	¿Permite a una aplicación M2M definir condiciones de activación en el sistema oneM2M de manera que envíe de forma autónoma una serie de comandos a actuadores en nombre de la aplicación M2M? ¿En qué módulo se gestiona?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/29	¿Puede enviar comandos a cada actuador o sensor de manera individual y/o en grupos? Indique si admite ambas formas
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/30	¿Realiza gestión de grupos (añadir, borrar, modificar y obtener)?
Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/31	¿Permite organizar grupos de grupos?
Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/32	¿Permite distintas categorías de eventos (normal, urgente) asociados con datos? ¿Cuáles?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/33	¿Ajusta dinámicamente la programación de informes y notificaciones de dispositivo/gateway M2M? ¿En que se basa?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/34	¿Permite el reemplazo sin interrupción de dispositivos y gateways?
Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/35	¿Permite el intercambio de información relevante de aplicaciones no-M2M (ej. Clases de dispositivos/gateways) con dispositivos/gateways M2M e infraestructuras de servicios M2M para el propósito de facilitar una comunicación eficiente?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/36	¿Acepta peticiones de aplicaciones proveedoras de servicios M2M para los servicios de cómputo/analíticas? Ponga un ejemplo.
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/37	¿Permite a una aplicación M2M solicitar el envío de datos, de una forma independiente de la red, a un grupo de dispositivos M2M y gateways M2M dentro de una zona geográfica?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/38	¿Soporta la inclusión de preferencias QoS (Quality of Service) de una aplicación M2M para peticiones de servicio a la red?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/39	¿Puede autorizar peticiones de servicio con preferencias QoS?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/40	¿Puede hacer uso de múltiples mecanismos de comunicación (tales como USSD o SMS) cuando estén disponibles en las redes? Cite algunos ejemplos
Si [ ] Respuesta:	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/41	¿Provee un mecanismo que soporta la adición de nuevos servicios M2M como módulos independientes conectados a través de las interfaces de oneM2M? ¿A través de que interfaz?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/42	¿Soporta diferentes parámetros de especificación de QoS tales como bit rate garantizado, retardo, variaciones de ratio de retardo de pérdidas, tasa de error? ¿Cuáles?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/43	¿Puede verificar que miembros de un grupo soportan una serie de funciones comunes? ¿Cómo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/44	¿Soporta comunicación con dispositivos M2M que son accesibles de forma programada y también con dispositivos M2M que son accesibles de una forma espontánea e impredecible?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/45a	¿Puede recibir y utilizar información obtenida de la red sobre cuando un dispositivo M2M puede ser accesible? ¿Cómo?
Si [ ] Respuesta:	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/45b	¿Puede utilizar horarios de accesibilidad generados tanto por el dispositivo M2M o por el Dominio de la Infraestructura? ¿En qué modulo se gestiona?
Si [ ] Respuesta:	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/46	¿Soporta la capacidad para que una aplicación M2M pueda requerir/rechazar un mecanismo de confirmación para sus comunicaciones?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/47	¿Soporta mecanismos para que los dispositivos M2M y/o Gateways informen sobre su localización geográfica a aplicaciones M2M? ¿En qué modulo se gestiona?
Si [ ] Respuesta:	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/48	¿Provee un servicio M2M que permite a dispositivos M2M y/o gateways compartir su información de localización geográfica o la de otros dispositivos M2M? ¿Cuál?
Si [ ] Respuesta:	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/49	¿Provee la capacidad para que una aplicación M2M pueda compartir datos entre Aplicaciones de forma selectiva? ¿Cómo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/50	Si la comunicación sobre un canal de comunicación provisto por la red solo puede ser activada unidireccionalmente (y hay canales alternativos disponibles en la otra dirección, ¿el sistema puede usar estos canales alternativos para activar la comunicación bidireccional en el primer canal?
Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/51	¿Puede pedir a la red que retransmita datos (broadcast / multicast) a un grupo de dispositivos M2M en un área específica?
Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/52	¿Puede seleccionar una red apropiada para hacer broadcast/multicast de datos dependiendo de las capacidades broadcast/multicast de la red y la conectividad soportada por el grupo elegido de dispositivos/gateways M2M?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/53	¿Permite la retrocompatibilidad de interfaces entre diferentes versiones?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/54	¿Permite que una aplicación M2M, un dispositivo M2M, o un gateway M2M obtengan acceso a los recursos de otra aplicación M2M, dispositivo M2M, o gateway M2M? Indique el flujo a seguir
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/55	¿Provee la capacidad de que las aplicaciones M2M intercambien datos con una o más aplicaciones M2M que no son conocidas por adelantado? ¿Cómo se gestiona?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/56	¿Permite el descubrimiento de las aplicaciones M2M de los gateways o dispositivos M2M? ¿Cómo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/57	¿Permite el descubrimiento de gateways y dispositivos M2M disponibles a una aplicación M2M para el intercambio de datos? ¿Cómo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/58	¿Provee marcas de tiempo para las funciones de los servicios comunes?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/59	¿Es capaz de permitir control de acceso basado en roles según las suscripciones a servicios M2M?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/60	¿Permite sincronización temporal con un reloj externo?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/61	¿Permite medios de testeo de la conectividad hacia una serie de aplicaciones M2M? ¿Cuáles?
Si [ ] Respuesta:	No [ ]

Otras observaciones:

ID	DESCRIPCIÓN
TP/M2M/OSR/62	¿Puede gestionar la planificación de la conectividad y mensajería entre el dominio de la infraestructura y los dispositivos/gateways M2M? ¿En qué módulo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/63	¿Puede agrupar mensajes dependiendo de la tolerancia al retardo y/o su categoría? ¿En qué módulo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/64	¿Provee mecanismos que permitan a un proveedor de servicios M2M distribuir funciones de procesado a sus dispositivos/gateways M2M? Ponga un ejemplo
Si [ ] No [ ] Respuesta:	

Otras observaciones:

ID	DESCRIPCIÓN
TP/M2M/OSR/65	¿Permite la colocación y operación de aplicaciones M2M en nodos M2M seleccionados según criterios requeridos por los proveedores de servicio, sujeto a los derechos de acceso? ¿En qué módulo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/66	¿Es capaz de tomar acciones de gestión y operación según lo requerido por las aplicaciones M2M? ¿En qué módulo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/67	Cuando esté disponible en una red, ¿Provee la capacidad de obtener y presentar la información en relación a si un

	dispositivo M2M está autorizado a acceder a los servicios de la red? ¿En qué módulo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/68	Cuando esté disponible en una red, ¿Mantiene el estado operacional del servicio M2M de un dispositivo M2M y lo actualizará cuando el estado del servicio de conectividad de la red cambie?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/69	¿Provee la capacidad de notificar a una aplicación M2M autorizada cuando el estado administrativo del servicio M2M o el estado operacional de un dispositivo M2M cambie, siempre que esa aplicación M2M esté suscrita a tales notificaciones?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/70	¿Permite a una aplicación M2M autorizada cambiar el estado administrativo de un servicio M2M en un dispositivo M2M?

Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OSR/71	¿Puede iniciar una serie de acciones bien definidas (activación si sobrepasa un umbral, comparar un valor, etc.) en una o más aplicaciones M2M en nombre de otra aplicación M2M? Ponga un ejemplo.
Si [ ] No [ ]	
Otras observaciones:	

REQUISITOS DE GESTIÓN

ID	DESCRIPCIÓN
TP/M2M/MGR/01	¿Soporta la gestión y la configuración de dispositivos/gateways OneM2M incluyendo recursos de los dispositivos oneM2M de capacidad reducida? Ponga un ejemplo.
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/MGR/02	¿Es capaz de descubrir redes que incluya información sobre dispositivos y los parámetros de esas redes (ej. topología, protocolo)? ¿En qué módulo?
Si [ ] No [ ]	

Respuesta:
Otras observaciones:

ID	DESCRIPCIÓN
TP/M2M/MGR/03	¿Es capaz de proveer la capacidad de mantener y describir el modelo de gestión de la información de los dispositivos y parámetros de redes M2M? ¿En qué módulo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/MGR/04	¿Soporta medios comunes de gestión de dispositivos que usan diferentes tecnologías de gestión (ej. OMA, DM, BBF TR069)? ¿Cuáles?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/MGR/05	¿Provee la capacidad de gestionar múltiples dispositivos de una manera agrupada?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/MGR/06	¿Provee la capacidad de suministrar y configurar dispositivos de redes M2M?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/MGR/07	¿Provee la capacidad de monitorización y diagnóstico de dispositivos/gateways en redes M2M?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/MGR/08	¿Provee la capacidad de gestión de software de los dispositivos en redes M2M?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/MGR/09	¿Provee la capacidad de reinicio y/o reseteo de dispositivos/gateways M2M y otros dispositivos en redes M2M?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/MGR/10	¿Provee la capacidad de autorizar a dispositivos el acceso a redes M2M?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/MGR/11	¿Provee la capacidad para modificar la topología de dispositivos en redes M2M, sujeto a restricciones basadas en las políticas de las redes M2M?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/MGR/12	¿Es capaz de proveer a un nuevo gateway detectado con una configuración adecuada (dada por la Infraestructura de servicios M2M) necesaria para manejar el dispositivo?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/MGR/14	¿Es capaz de recuperar eventos e información enviada por gateways/dispositivos M2M y otros dispositivos en redes M2M?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/MGR/15	¿Es capaz de gestionar firmware de gateways/dispositivos M2M y otros dispositivos en redes M2M?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/MGR/16	¿Es capaz de recuperar información relativa al contexto dinámico y estático de dispositivos/gateways M2M?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/MGR/17	¿Es capaz de relacionar elementos de gestión de acceso proporcionados por los protocolos de gestión de la tecnología específica del dispositivo con los elementos de gestión de acceso del sistema? ¿En qué módulo?
Si [ ]	No [ ]

Respuesta:
Otras observaciones:

REQUISITOS DE ABSTRACCIÓN

ID	DESCRIPCIÓN
TP/M2M/ABR/01	¿Define la estructura de un modelo de Información con el propósito de intercambiar datos? ¿Cuál?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/ABR/02	¿Provee mecanismos de traducción entre Modelos de Información usados por las distintas Aplicaciones y dispositivos/gateways M2M y otros dispositivos? ¿Cuáles?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/ABR/03	¿Proporciona capacidades para representar dispositivos y objetos virtuales? Ponga un ejemplo
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

REQUISITOS SEMÁNTICOS

ID	DESCRIPCIÓN
TP/M2M/SMR/01	¿Provee capacidades para gestionar información semántica sobre los recursos oneM2M (crear, recuperar, modificar, borrar, asociar)?
Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SMR/02	¿Soporta un sistema de modelado común de descripciones semánticas (incluyendo relaciones entre objetos) para que puedan ser usadas por Aplicaciones M2M)?¿Cuál?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SMR/03	¿Provee capacidades de cooperación entre diferentes lenguajes de modelado para las descripciones semánticas?¿Qué lenguajes?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SMR/04	¿Provee capacidades para de descubrimiento de Recursos M2M basados en descripciones semánticas?
Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SMR/05	¿Soporta el acceso a descripciones semánticas externas al sistema OneM2M?¿Cuáles?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SMR/06	¿Es capaz de realizar análisis de datos M2M basados en

	descripciones semánticas de aplicaciones M2M y/o del sistema OneM2M?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SMR/07	¿Es capaz de realizar Mash-up semánticos usando datos M2M de Aplicaciones M2M y/o del sistema OneM2M (ej. Crear Dispositivos Virtuales, ofrecer nuevos servicios M2M, etc…).?
Si [ ]	No [ ]
Otras observaciones:	

REQUISITOS DE SEGURIDAD

ID	DESCRIPCIÓN
TP/M2M/SER/01	¿Incorpora mecanismos contra amenazas tales como ataques DoS (Denial of Service)?¿Cuáles?
Si [ ] Respuesta:	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SER/02	¿Es capaz de asegurar la confidencialidad de los datos?¿Cómo?
Si [ ] Respuesta:	No [ ]

Otras observaciones:

ID	DESCRIPCIÓN
TP/M2M/SER/03	¿Es capaz de asegurar la integridad de los datos?¿Cómo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SER/04	En casos donde el dispositivo M2M soporte USIM/UICC y las redes soporten seguridad en la capa de red, (ej. 3GPP GBA) para establecer el nivel de seguridad a través de interfaces a la red de las aplicaciones y servicios M2M ¿Se utilizan para establecer el nivel de seguridad?.
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SER/05	¿El sistema oneM2M es capaz de exponer sus capacidades a servicios M2M a través de APIs, si el dispositivo soporta USIM/UICC y la red soporta seguridad en la capa de red?
Si [ ]	No [ ]

Otras observaciones:

ID	DESCRIPCIÓN
TP/M2M/SER/06	¿El sistema oneM2M es capaz de hacer uso de las credenciales USIM/UICC del dispositivo cuando sea posible para bootstrap la asociación de seguridad?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SER/07	Cuando algunos de los componentes de una solución M2M no estén disponibles (ej. pérdida de conexión con una WAN), ¿se permite la confidencialidad e integridad de los datos entre componentes autorizados de la solución M2M que estén disponibles?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SER/08	¿Tiene medidas contra el acceso no autorizado a servicios M2M y servicios de aplicación M2M? ¿Cuáles?
Si [ ] No [ ] Respuesta:	

Otras observaciones:

ID	DESCRIPCIÓN
TP/M2M/SER/09	¿Soporta autentificación mutua para la interacción con redes, servicios M2M y servicios de aplicaciones M2M?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SER/10	¿Incorpora mecanismos para la protección contra el uso indebido, clonado, sustitución o robo de credenciales de seguridad? ¿Cuáles?
Si [ ] Respuesta:	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SER/11	¿Protege el uso de la identidad de un cliente M2M dentro del sistema contra el descubrimiento y uso indebido por otros clientes? ¿Cómo?
Si [ ] Respuesta:	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SER/12	¿Incorpora medidas contra ataques de suplantación y de retransmisión? ¿Cuáles?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SER/13	¿Provee mecanismos para comprobar la integridad al arranque y periódicamente en run-time sobre componentes de software/hardware/firmware en dispositivos M2M? ¿Cuáles?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SER/14	¿Provee datos de configuración a una aplicación autenticada y autorizada del dispositivo/gateway M2M?
Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SER/15	¿Provee mecanismos para proveer identidades de suscriptores a aplicaciones M2M autorizadas y autenticadas cuando el sistema tiene el consentimiento del suscriptor? ¿En qué módulo?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SER/16	¿Soporta procedimientos de no repudio (non repudiation) dentro de la capa de servicio M2M y sus interacciones autorizadas con la red y las capas de aplicación?
Si [ ] No [ ] Respuesta:	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SER/17	¿Es capaz de mitigar amenazas identificadas en el documento oneM2M TR-0008?
Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SER/18	¿Permite a un cliente M2M usar un recurso o servicio y es responsable de ese uso sin exponer su identidad a otros clientes?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SER/19	¿Puede usar credenciales a nivel de servicio dentro del dispositivo M2M para establecer el nivel de seguridad de aplicaciones y servicios M2M?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SER/20	¿Permite a los proveedores de servicio M2M legítimos provisionar sus propias credenciales en los dispositivos/gateways M2M?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SER/21	¿Puede, de forma remota y segura, provisionar credenciales de seguridad M2M en dispositivos/gateways M2M?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SER/22	¿Permite a los proveedores de servicio de aplicaciones M2M a autorizar interacciones que involucren a sus aplicaciones M2M y a dispositivos y gateways?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SER/23	¿El sistema oneM2M usa HSM (Hardware Security Module) para proveer seguridad local?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SER/24	¿Permite a aplicaciones M2M el uso de entornos de seguridad diferentes y separados?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/SER/25	¿Incorpora mecanismos de prevención frente a clientes M2M desautorizados de identificar y/o observar las acciones de otros clientes?
Si [ ]	No [ ]

Otras observaciones:

ID	DESCRIPCIÓN
TP/M2M/SER/26	¿Provee mecanismos para la protección de la confidencialidad de la información geográfica?
Si [ ]	No [ ]
Otras observaciones:	

REQUISITOS DE TARIFICACIÓN

IID	DESCRIPCIÓN
TP/M2M/CHG/01	¿Soporta recopilación de información específica de tarificación relacionada con los servicios individuales?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/CHG/02	¿Soporta mecanismos para facilitar la correlación de información de tarificación recopilada?
Si [ ]	No [ ]
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/CHG/03	¿Proporciona medios para coordinar los registros de datos de tarificación para diferentes QoS de la red?

Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/CHG/04	¿Puede utilizar mecanismos existentes de tarificación de la red?
Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/CHG/05	¿Proporciona transferencia de los registros de información de tarificación al dominio de facturación del proveedor de servicio M2M incluyendo funciones adicionales como estadísticas?
Si [ ] No [ ]	
Otras observaciones:	

ID	DESCRIPCIÓN
TP/M2M/CHG/06	¿Permite la generación de eventos de tarificación con el propósito de solicitar autorización de uso de recursos del sistema de control de crédito en tiempo real donde esté la cuenta del suscriptor?
Si [ ] No [ ]	
Otras observaciones:	

REQUISITOS OPERACIONALES

ID	DESCRIPCIÓN
TP/M2M/OPR/01	¿Proporciona la capacidad para monitorización y diagnóstico de aplicaciones M2M? ¿En qué módulo?
Si [ ] No [ ] Respuesta:	
Otras Observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OPR/02	¿Proporciona la capacidad de gestión de software de aplicaciones M2M? ¿En qué módulo?
Si [ ] No [ ] Respuesta:	
Otras Observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OPR/03	¿Proporciona la capacidad de configurar el estado de ejecución de aplicaciones M2M (start, stop, restart)? ¿En qué módulo?
Si [ ] No [ ] Respuesta:	
Otras Observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OPR/04	¿Tiene la habilidad de programar el tráfico a través de la red basándose en instrucciones recibidas de la propia red? ¿En qué módulo?
Si [ ] No [ ] Respuesta:	
Otras Observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OPR/05	¿Tiene la capacidad de intercambiar, con aplicaciones M2M, información relacionada con las características de uso y tráfico de los dispositivos/gateways M2M?
Si [ ]	No [ ]
Otras Observaciones:	

ID	DESCRIPCIÓN
TP/M2M/OPR/06	¿Tiene la capacidad de intercambiar, con aplicaciones M2M, información relacionada con las características de uso y tráfico de los dispositivos/gateways M2M?
Si [ ]	No [ ]
Otras Observaciones:	

REQUISITOS DE GESTIÓN DE LA COMUNICACIÓN

ID	DESCRIPCIÓN
TP/M2M/CMR/01	¿Proporciona un servicio de comunicación que incluye buffering de los mensajes a/desde gateways, dispositivos o dominio de la infraestructura M2M?
Si [ ]	No [ ]
Otras Observaciones:	

ID	DESCRIPCIÓN
TP/M2M/CMR/02	¿Es capaz de reenviar los mensajes en buffer según las políticas de comunicaciones y basándose en las preferencias del servicio?
Si [ ]	No [ ]
Otras Observaciones:	

ID	DESCRIPCIÓN
TP/M2M/CMR/03	¿Permite a una aplicación M2M el envío de una petición de comunicación con las siguientes preferencias de servicio: • Parámetros QoS, incluyendo tolerancia al retardo, para iniciar la entrega de datos. • Categorización de las peticiones de comunicación en diferentes niveles de prioridad o clases de QoS?
Si [ ]	No [ ]
Otras Observaciones:	

ID	DESCRIPCIÓN
TP/M2M/CMR/04	¿Soporta el procesado concurrente de mensajes dentro de los gateways y/o dispositivos M2M de diferente origen y con conocimiento de la preferencia de servicio asociada a los mensajes, teniendo en cuenta las políticas de comunicación proporcionadas?
Si [ ]	No [ ]
Otras Observaciones:	

ID	DESCRIPCIÓN
TP/M2M/CMR/05	¿Mantiene un contexto asociado a las sesiones M2M (ej. contexto de seguridad o conectividad de red durante la interrupción de la sesión)?
Si [ ]	No [ ]
Otras Observaciones:	

3.6. MÉTRICAS

3.6.1. MÉTRICAS PARA LA UNE 178 104

Las métricas definidas en el documento de referencia son las siguientes:

a. Grado de adecuación al modelo de capas y funcionalidades

b. Modularidad de la Plataforma.

c. Integración con otras Plataformas.

d. Basarse en estándares abiertos.

e. Protocolos IoT soportados.

f. Capacidad de extensión de la Plataforma.

g. Soporte Enfoque Big Data

h. Soporte Enfoque Opendata

i. Servicio en On premise/cloud.

j. Inclusión capacidades GIS.

k. Inclusión de herramientas de uso y configuración.

l. Niveles de disponibilidad y nivel de servicio

m. Garantía, soporte y hoja de ruta

A continuación se propone una **modificación de este conjunto de métricas** en base a los requisitos extraídos, dando como resultado el siguiente conjunto de métricas:

a. Gestión de datos y activos

b. Herramientas de uso, configuración, DSS y mantenimiento

c. Gestión de dispositivos y gateways

d. Herramientas para desarrollo de apps

e. Publicación de información

f. Integración con otros sistemas

g. Protocolos IoT soportados

h. Estándares abiertos y Semántica

i. Seguridad, privacidad y confidencialidad

j. Mantenimiento, garantía, soporte y hoja de ruta

k. Niveles de disponibilidad y servicio

l. Arquitectura de capas funcionales

m. Capacidad de extensión y modularidad

A cada métrica se han asociado un conjunto de cuestiones relacionadas. Así mismo, hay cuestiones que se considera que pueden tener un impacto mayor o menor en la adecuación de las Plataformas con los objetivos que se persiguen en este estudio. Por esta razón, el peso de cada cuestión es diferente.

Para el cálculo del valor final asociado a cada una de las métricas, se considerarán aquellas cuestiones a las que se ha respondido afirmativamente y se ha justificado dicha respuesta (en caso contrario será 0). El valor final se calcula realizando la suma de todos los porcentajes de las preguntas consideradas como positivas.

A continuación se muestran los pesos de cada cuestión para la métrica correspondiente asociada.

a. **Gestión de datos y activos**

Cuestión	Peso
TP/UNE/RFUN/REP/01	7,5%
TP/UNE/RFUN/REP/02	5%
TP/UNE/RFUN/REP/05	7,5%
TP/UNE/RFUN/INFR/01	7,5%
TP/UNE/RFUN/SEC/10	7,5%
TP/UNE/RFUN/DSS/04	7,5%
TP/UNE/RFUN/PUBL/01	7,5%
TP/UNE/RTEC/11	7,5%
TP/UNE/ARQ/CON/01	7,5%
TP/UNE/ARQ/CON/02	7,5%
TP/UNE/ARQ/CON/03	7,5%
TP/UNE/ARQ/CON/04	7,5%
TP/UNE/ARQ/CON/05	7,5%
TP/UNE/ARQ/SOP/02	5%

b. Herramientas de uso, configuración, DSS

Cuestión	Peso
TP/UNE/RFUN/REP/03	5%
TP/UNE/RFUN/SEC/06	5%

TP/UNE/RFUN/APP/01	5%
TP/UNE/RFUN/APP/02	5%
TP/UNE/RFUN/APP/03	5%
TP/UNE/RFUN/APP/05	5%
TP/UNE/RFUN/APP/06	5%
TP/UNE/RFUN/APP/07	5%
TP/UNE/RFUN/DSS/01	5%
TP/UNE/RFUN/DSS/02	5%
TP/UNE/RFUN/DSS/03	5%
TP/UNE/RFUN/DSS/04	5%
TP/UNE/RFUN/DSS/05	5%
TP/UNE/RTEC/15	5%
TP/UNE/ARQ/CON/03	5%
TP/UNE/ARQ/CON/05	5%
TP/UNE/ARQ/CINT/04	5%
TP/UNE/ARQ/SER/01	5%
TP/UNE/ARQ/SER/02	5%
TP/UNE/ARQ/SOP/01	5%

c. Gestión de dispositivos y gateways

Cuestión	Peso
TP/UNE/RFUN/INFR/02	10%
TP/UNE/RFUN/INT/03	10%
TP/UNE/RFUN/SEC/11	10%
TP/UNE/RTEC/02	10%
TP/UNE/RTEC/03	10%
TP/UNE/ARQ/ADQ/02	10%
TP/UNE/ARQ/ADQ/04	10%
TP/UNE/ARQ/ADQ/06	10%
TP/UNE/ARQ/ADQ/07	10%
TP/UNE/ARQ/ADQ/08	10%

d. Herramientas para desarrollo de apps

Cuestión	Peso
TP/UNE/RFUN/APP/01	20%
TP/UNE/RFUN/APP/02	10%
TP/UNE/ARQ/ADQ/04	35%
TP/UNE/ARQ/CINT/05	35%

e. Publicación de información

Cuestión	Peso

TP/UNE/RFUN/APP/01	12%
TP/UNE/RFUN/PUBL/01	12%
TP/UNE/RFUN/PUBL/02	12%
TP/UNE/RFUN/PUBL/04	12%
TP/UNE/RFUN/PUBL/05	12%
TP/UNE/RFUN/PUBL/06	12%
TP/UNE/RFUN/PUBL/07	4%
TP/UNE/ARQ/CINT/01	12%
TP/UNE/ARQ/CINT/04	12%

f. Integración con otros sistemas

Cuestión	Peso
TP/UNE/RFUN/REP/04	3%
TP/UNE/RFUN/INFR/06	4%
TP/UNE/RFUN/INT/01	4%
TP/UNE/RFUN/SEC/08	4%
TP/UNE/RFUN/MANT/03	4%
TP/UNE/RFUN/DSS/05	4%
TP/UNE/RFUN/PUBL/05	4%
TP/UNE/RFUN/PUBL/06	4%

TP/UNE/RTEC/02	15%
TP/UNE/ARQ/CINT/01	15%
TP/UNE/ARQ/CINT/02	15%
TP/UNE/ARQ/CINT/03	15%
TP/UNE/IPL/01	3%
TP/UNE/IPL/02	3%
TP/UNE/IPL/03	3%

g. Protocolos IoT soportados

Cuestión	Peso
TP/UNE/RFUN/INFR/02	25%
TP/UNE/RFUN/INT/03	25%
TP/UNE/ARQ/ADQ/07	25%
TP/UNE/ARQ/ADQ/09	12,5%
TP/UNE/ARQ/CINT/06	12,5%

h. Estándares abiertos y Semántica

Cuestión	Peso
TP/UNE/RFUN/INT/02	13%
TP/UNE/RTEC/02	13%
TP/UNE/RTEC/12	13%

TP/UNE/RTEC/13	9%
TP/UNE/RTEC/16	13%
TP/UNE/ARQ/ADQ/03	13%
TP/UNE/ARQ/CON/08	13%
TP/UNE/ARQ/CINT/01	13%

i. Seguridad, privacidad y confidencialidad

Cuestión	Peso
TP/UNE/RFUN/INFR/03	2%
TP/UNE/RFUN/SEC/01	8%
TP/UNE/RFUN/SEC/02	8%
TP/UNE/RFUN/SEC/03	8%
TP/UNE/RFUN/SEC/04	8%
TP/UNE/RFUN/SEC/05	8%
TP/UNE/RFUN/SEC/06	2%
TP/UNE/RFUN/SEC/07	4%
TP/UNE/RFUN/SEC/08	4%
TP/UNE/RFUN/SEC/09	4%
TP/UNE/RFUN/SEC/10	8%
TP/UNE/RFUN/SEC/11	8%

TP/UNE/RFUN/SEC/12	8%
TP/UNE/RTEC/17	8%
TP/UNE/ARQ/CON/07	8%
TP/UNE/ARQ/SOP/03	4%

j. Mantenimiento, garantía, soporte y hoja de ruta

Cuestión	Peso
TP/UNE/RFUN/INFR/04	18%
TP/UNE/RFUN/INFR/05	18%
TP/UNE/RFUN/MANT/01	18%
TP/UNE/RFUN/MANT/02	18%
TP/UNE/RFUN/MANT/03	18%
TP/UNE/RFUN/MANT/04	10%

k. Niveles de disponibilidad y servicio

Cuestión	Peso
TP/UNE/RFUN/APP/04	5%
TP/UNE/RFUN/PUBL/03	5%
TP/UNE/RFUN/FALL/01	15%
TP/UNE/RFUN/FALL/02	15%
TP/UNE/RTEC/05	15%

TP/UNE/RTEC/07	15%
TP/UNE/RTEC/08	15%
TP/UNE/ARQ/SER/03	15%

I. Arquitectura de capas funcionales

Cuestión	Peso
TP/UNE/ARQ/01	8%
TP/UNE/ARQ/ADQ/01	4%
TP/UNE/ARQ/ADQ/02	4%
TP/UNE/ARQ/ADQ/03	2%
TP/UNE/ARQ/ADQ/04	4%
TP/UNE/ARQ/ADQ/05	2%
TP/UNE/ARQ/ADQ/06	2%
TP/UNE/ARQ/ADQ/07	4%
TP/UNE/ARQ/ADQ/08	2%
TP/UNE/ARQ/CON/01	4%
TP/UNE/ARQ/CON/02	4%
TP/UNE/ARQ/CON/03	4%
TP/UNE/ARQ/CON/04	4%
TP/UNE/ARQ/CON/05	4%

TP/UNE/ARQ/CON/06	4%
TP/UNE/ARQ/CON/07	4%
TP/UNE/ARQ/CON/08	4%
TP/UNE/ARQ/CINT/01	4%
TP/UNE/ARQ/CINT/02	4%
TP/UNE/ARQ/CINT/03	3%
TP/UNE/ARQ/CINT/04	3%
TP/UNE/ARQ/CINT/05	4%
TP/UNE/ARQ/CINT/06	2%
TP/UNE/ARQ/SER/01	4%
TP/UNE/ARQ/SER/02	2%
TP/UNE/ARQ/SER/03	3%
TP/UNE/ARQ/SOP/01	2%
TP/UNE/ARQ/SOP/02	2%
TP/UNE/ARQ/SOP/03	3%

m. Capacidad de extensión y modularidad

Cuestión	Peso
TP/UNE/RTEC/01	10%
TP/UNE/RTEC/04	16%

TP/UNE/RTEC/06	16%
TP/UNE/RTEC/09	10%
TP/UNE/RTEC/10	16%
TP/UNE/RTEC/13	16%
TP/UNE/RTEC/14	16%

3.6.2. MÉTRICAS PARA TS-0001

De la misma forma que para la UNE, a continuación se definen las cuestiones asociadas y los pesos para cada una de las métricas para evaluar el cumplimiento del TS-0001 oneM2M [3].

De cara una mejor operativa de verificación, se han definido las siguientes métricas a las que se asocian las cuestiones relativas a los diferentes requisitos extraídos de la TS-0001 [3].

Las métricas definidas son las siguientes:

a. Generales
b. Registro
c. Gestión de datos
d. Suscripción y notificación
e. Gestión de grupos
f. Descubrimiento
g. Gestión de la localización
h. Gestión de dispositivos
i. Gestión de las comunicaciones y de entregas
j. Seguridad
k. Tarificación

A continuación las cuestiones y pesos asociados a cada una de las métricas.

a. Generales

Cuestión	Peso
TP/M2M/OSR/01	8%
TP/M2M/OSR/06	5%
TP/M2M/OSR/22	8%
TP/M2M/OSR/34	8%
TP/M2M/OSR/53	8%
TP/M2M/OSR/58	8%
TP/M2M/OSR/60	8%
TP/M2M/OSR/63	5%
TP/M2M/OSR/65	6%
TP/M2M/OPR/01	8%
TP/M2M/OPR/02	8%
TP/M2M/OPR/03	8%
TP/M2M/OPR/05	6%
TP/M2M/OPR/06	6%

b. Registro

Cuestión	Peso
TP/M2M/OSR/23	11%
TP/M2M/OSR/24	11%

TP/M2M/OSR/25	11%
TP/M2M/OSR/26	11%
TP/M2M/OSR/28	11%
TP/M2M/OSR/29	11%
TP/M2M/OSR/55	10%
TP/M2M/MGR/10	12%
TP/M2M/MGR/12	12%

c. Gestión de datos

Cuestión	Peso
TP/M2M/OSR/07	4,25%
TP/M2M/OSR/17	4,25%
TP/M2M/OSR/19	5%
TP/M2M/OSR/20	5%
TP/M2M/OSR/21	5%
TP/M2M/OSR/27	5%
TP/M2M/OSR/36	4,25%
TP/M2M/OSR/49	5%
TP/M2M/OSR/55	4,25%
TP/M2M/MGR/03	4,25%

TP/M2M/MGR/16	4,25%
TP/M2M/ABR/01	7%
TP/M2M/ABR/02	5%
TP/M2M/ABR/03	4,25%
TP/M2M/SMR/01	5%
TP/M2M/SMR/02	7%
TP/M2M/SMR/03	5%
TP/M2M/SMR/05	4,25%
TP/M2M/SMR/06	7%
TP/M2M/SMR/07	5%

d. Suscripción y notificación

Cuestión	Peso
TP/M2M/OSR/16	5%
TP/M2M/OSR/28	5%
TP/M2M/OSR/29	3%
TP/M2M/OSR/32	5%
TP/M2M/OSR/33	5%
TP/M2M/OSR/45a	9%
TP/M2M/OSR/45b	8%

TP/M2M/OSR/46	5%
TP/M2M/OSR/49	8%
TP/M2M/OSR/59	9%
TP/M2M/OSR/65	5%
TP/M2M/OSR/68	8%
TP/M2M/OSR/69	8%
TP/M2M/OSR/70	8%
TP/M2M/OSR/71	9%

e. Gestión de grupos

Cuestión	Peso
TP/M2M/OSR/30	20%
TP/M2M/OSR/31	10%
TP/M2M/OSR/43	20%
TP/M2M/OSR/51	20%
TP/M2M/OSR/52	10%
TP/M2M/MGR/05	20%

f. Descubrimiento

Cuestión	Peso
TP/M2M/OSR/05	20%

TP/M2M/OSR/54	20%
TP/M2M/OSR/56	20%
TP/M2M/OSR/57	20%
TP/M2M/SMR/04	20%

g. Gestión de la localización

Cuestión	Peso
TP/M2M/OSR/37	40%
TP/M2M/OSR/47	30%
TP/M2M/OSR/48	30%

h. Gestión de dispositivos

Cuestión	Peso
TP/M2M/OSR/02a	4%
TP/M2M/OSR/02b	4%
TP/M2M/OSR/08	2%
TP/M2M/OSR/09	4%
TP/M2M/OSR/14	4%
TP/M2M/OSR/16	4%
TP/M2M/OSR/17	2,5%
TP/M2M/OSR/18	2,5%

TP/M2M/OSR/35	2,5%
TP/M2M/OSR/44	4%
TP/M2M/OSR/45a	4%
TP/M2M/OSR/64	2,5%
TP/M2M/OSR/66	2,5%
TP/M2M/OSR/67	4%
TP/M2M/MGR/01	4%
TP/M2M/MGR/02	2,5%
TP/M2M/MGR/03	4%
TP/M2M/MGR/04	2,5%
TP/M2M/MGR/05	2,5%
TP/M2M/MGR/06	2,5%
TP/M2M/MGR/07	3,5%
TP/M2M/MGR/08	2,5%
TP/M2M/MGR/09	2,5%
TP/M2M/MGR/10	4%
TP/M2M/MGR/11	2,5%
TP/M2M/MGR/12	2,5%
TP/M2M/MGR/14	4%

TP/M2M/MGR/15	2,5%
TP/M2M/MGR/16	2,5%
TP/M2M/MGR/17	2,5%
TP/M2M/OPR/05	4%
TP/M2M/OPR/06	2,5%

i. Gestión de las comunicaciones y de entregas

Cuestión	Peso
TP/M2M/OSR/02a	3%
TP/M2M/OSR/02b	3%
TP/M2M/OSR/03	2%
TP/M2M/OSR/04	2%
TP/M2M/OSR/08	2%
TP/M2M/OSR/09	3%
TP/M2M/OSR/10	2%
TP/M2M/OSR/11a	2%
TP/M2M/OSR/11b	2%
TP/M2M/OSR/12	3%
TP/M2M/OSR/13	2%
TP/M2M/OSR/14	3%

TP/M2M/OSR/15	3%
TP/M2M/OSR/17	3%
TP/M2M/OSR/18	2%
TP/M2M/OSR/35	2%
TP/M2M/OSR/38	2%
TP/M2M/OSR/39	2%
TP/M2M/OSR/40	3%
TP/M2M/OSR/41	4%
TP/M2M/OSR/42	2%
TP/M2M/OSR/44	3%
TP/M2M/OSR/50	2%
TP/M2M/OSR/51	3%
TP/M2M/OSR/52	3%
TP/M2M/OSR/54	5%
TP/M2M/OSR/61	3%
TP/M2M/OSR/62	5%
TP/M2M/CMR/01	5%
TP/M2M/CMR /02	5%
TP/M2M/CMR /03	5%

TP/M2M/CMR /04	3%
TP/M2M/CMR /05	3%
TP/M2M/OPR/04	3%

j. Seguridad

Cuestión	Peso
TP/M2M/SER/01	3%
TP/M2M/SER/02	5%
TP/M2M/SER/03	5%
TP/M2M/SER/04	3%
TP/M2M/SER/05	3%
TP/M2M/SER/06	3%
TP/M2M/SER/07	4%
TP/M2M/SER/08	4%
TP/M2M/SER/09	4%
TP/M2M/SER/12	4%
TP/M2M/SER/11	4%
TP/M2M/SER/12	4%
TP/M2M/SER/13	3%
TP/M2M/SER/14	4%

TP/M2M/SER/15	4%
TP/M2M/SER/16	4%
TP/M2M/SER/17	4%
TP/M2M/SER/18	4%
TP/M2M/SER/19	4%
TP/M2M/SER/20	4%
TP/M2M/SER/21	4%
TP/M2M/SER/22	4%
TP/M2M/SER/23	3%
TP/M2M/SER/24	4%
TP/M2M/SER/25	4%
TP/M2M/SER/26	4%

k. Tarificación

Cuestión	Peso
TP/M2M/CHG/01	20%
TP/M2M/CHG/02	20%
TP/M2M/CHG/03	10%
TP/M2M/CHG/04	10%
TP/M2M/CHG/05	20%

TP/M2M/CHG/06	20%

4. ACRÓNIMOS

3GPP	*3rd Generation Partnership Project*
AEN/CTN	*Comité Técnico de Normalización de AENOR*
API	*Application Programming Interface*
APP	*Application*
BBF	*Broadband forum*
CPU	*Central processing unit*
DM	*Device management*
DSS	*Decision Support System*
ETL	*Extract, Transform and Load*
GR	*Grupo*
GSMA	*Groupe Speciale Mobile Association*
IP	*Internet Protocol*
JMX	*Java Management Extensions*
LDAP	*Lightweight Directory Access Protocol*
M2M	*Machine to Machine communications*
OMA	*Open Mobile Alliance*
QoS	*Quality of Service*
REST	*Representational State Transfer*
SCADA	*Supervisory Control And Data Acquisition*
SDK	*software development kit*
SGR	*Subgrupo*
SLA	*Service Level Agreement*
SMS	*Short Message Service*
SNMP	*Simple Network Management Protocol*
TR	*Technical report*
TS	*Technical specification*
UICC	*Universal Integrated Circuit Card*
UNE	*Una Norma Española*
USIM	*Universal Subscriber Identity Module*

USSD	*Unstructured Supplementary Service Data*
XML	*eXtensible Markup Language*
WAN	*Wide Area Network*

5. REFERENCIAS

[1] UNE 178 104 Ciudades Inteligentes (AENOR). Infraestructuras. “Sistemas integrales de gestión de la Ciudad Inteligente”

[2] UNE 178 301 (AENOR). “Ciudades Inteligentes. Datos abiertos”

[3] TS-0001 (oneM2M). “Functional Architecture”. V1.6.1

[4] TS-0002 (oneM2M). “Requirements” V1.0.1

[5] TR-0001 (oneM2M). “oneM2M Use Cases Collection” V0.0.5

[6] Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes. Red.es. Introducción.

[7] Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes. Red.es. PARTE 2: Metodología.

[8] Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes. Red.es. PARTE 2: Metodología. ANEXO confidencial.

[9] Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes. Red.es. PARTE 4: Soluciones Alternativas.

Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes

PARTE 4: SOLUCIONES ALTERNATIVAS

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO
ontsi observatorio nacional de las telecomunicaciones y de la SI

Este documento constituye una aproximación parcial al estudio de la interoperabilidad en nuestras ciudades; se enmarca dentro del *Servicio para el Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes* promovido por el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información, de Red.es, y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la información.

Para la realización de este estudio se ha contado con la colaboración de AT4 wireless S.A.U.

Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes

Año 2016

ÍNDICE

1. RESUMEN EJECUTIVO

La interoperabilidad es un elemento central en el desarrollo de las Ciudades Inteligentes. El Comité Técnico de Normalización AEN/CTN 178 "Ciudades inteligentes" movilizó un amplio consenso en la redacción de la norma: "Ciudades inteligentes. Infraestructuras. Sistemas Integrales de Gestión de la Ciudad Inteligente" (UNE 178 104)[3].

El presente estudio constituye una primera aproximación al conocimiento del concepto de interoperabilidad entre plataformas de gestión de servicios inteligentes. Se trata, por tanto, de un estudio parcial ya que está centrado en estándares que no tienen exactamente el mismo objeto, puesto que la Norma UNE 178 104 es más específica para la materia que el estándar oneM2M. Desde el Plan Nacional de Ciudades Inteligentes está previsto definir estudios que aborden con mayor profundidad los casos de aplicación que se consideren relevantes.

Este documento constituye el último de los cuatro de los que se compone dicho estudio y recoge una serie de propuestas de fomento de la interoperabilidad en el ecosistema de Ciudades Inteligentes nacional.

Como primer punto, se recomiendan una serie de acciones inmediatas y transitorias de cara al fomento de la interoperabilidad en base a los resultados del análisis de casos de uso sobre las Plataformas consideradas en este Estudio.

A continuación, en los apartados siguientes, se proponen una serie de alternativas generales que pueden fomentar la interoperabilidad en los despliegues de Ciudades Inteligentes en línea con el Plan Nacional de Ciudades Inteligentes. Son las siguientes:

1. De manera provisional, con el objetivo final de alcanzar el cumplimiento con oneM2M, se considera el desarrollo de nuevos elementos: "**crawlers**" que adapten desde el punto de vista semántico los datos intercambiados entre las Plataformas, los sensores y aplicaciones o **gateways** que hagan de pasarelas adaptando tanto los datos como la conectividad de dispositivos [11].

2. Por otro lado, se estima que el desarrollo y difusión de una **Guía de diseño** que colabore al acercamiento a los estándares tanto de Plataformas como de dispositivos y aplicaciones en la que se defina el desarrollo de nuevas interfaces adaptadas al estándar.

3. Otro paso hacia el aprovechamiento de los desarrollos actuales es potenciar el Interfuncionamiento (interworking) entre Plataformas, para ello será necesario el desarrollos de nuevos elementos, propuestos por el oneM2M, llamados **IPE** (Interworking Proxy Entity) [11].

4. Finalmente, el cumplimiento con los estándares oneM2M y la **verificación formal** del mismo por parte de Plataformas, aplicaciones y dispositivos garantizará la convergencia de todos los elementos en un ecosistema abierto, inteligente e interoperable.

Adicionalmente a los aspectos técnicos tratados en los apartados anteriores se enumeran a continuación una serie de acciones que potenciarían alcanzar los objetivos

finales de promover la tecnología más adecuada y competitiva dentro de la industria de Tecnologías de la Información y las Comunicaciones nacional.

Acciones a nivel normativo

Por particular relevancia, se detallan aquí recomendaciones concretas en materia de normativa y certificación.

1. En este Estudio se han desarrollado auto-cuestionarios de cumplimiento con las normas UNE 178 104 [3] y oneM2M TS-0001 [8]. Para hacer más fácilmente accesible para todas las empresas interesadas, se propone el desarrollo de una Web donde se puedan completar estos cuestionarios, de manera que la evaluación del grado de cumplimiento se realice automáticamente asignando los resultados para las métricas definidas y de esta manera realizar recomendaciones sobre la hoja de ruta de los productos o acciones específicas según los resultados obtenidos.

2. Uno de los aspectos que pueden ocasionar más problemas a la hora de conseguir la interoperabilidad son los aspectos semánticos. Se recomienda definir un nuevo estándar que recoja claramente un único vocabulario semántico común para todas las Plataformas, dispositivos y apps que se vayan a utilizar en el despliegue de Servicios de las Ciudades Inteligentes en España.

3. Se propone, de cara a acelerar el cumplimiento con los estándares que está promoviendo AENOR en materia de Ciudades Inteligentes, la realización de eventos plugfest para Plataformas y productos Smart Cities (sensores, apps, etc.). Normalmente, estos eventos de interoperabilidad reúnen a diferentes proveedores (a menudo competidores) con el fin de comprobar si sus productos aplican correctamente las normas y son interoperables entre sí. Este enfoque ha demostrado ser una práctica manera de impulsar la interoperabilidad más para el desarrollo de normas, y se ha aplicado con cierto éxito por organizaciones de normalización así como por los consorcios de la industria. Se recomienda un primer evento antes del fin del primer semestre de 2016 y un segundo evento en septiembre-octubre de 2016. Como ejemplo, oneM2M ha organizado uno de estos eventos para la norma TS-0001 en septiembre de 2015 [15], de manera muy satisfactoria, y tiene previsto el próximo evento en mayo de 2016.

4. Realizar Estudios adicionales y de mayor profundidad respecto a casos de uso que tienen mayor despliegue real en las ciudades españolas.

Acciones a Nivel de capacitación del empleo y competitividad

De cara a mejorar el nivel de conocimiento y capacitación de la industria TIC nacional y así aumentar la competitividad se proponen las siguientes acciones:

5. Elaboración de Guías para desarrolladores de productos y servicios de Ciudades inteligentes, proporcionando información y herramientas técnicas para que los desarrollos cumplan con las normas obligatorias (marcado CE, LOPD, etc.) y con los nuevos estándares que van a dar mejoras competitivas a sus productos frente a los mercados nacionales e internacionales.

6. Fomentar la formación y difusión en materia de estandarización, interoperabilidad e industrialización de productos y soluciones de Ciudades

Inteligentes tanto para desarrolladores como a la administración pública que actúa como cliente.

Acciones a Nivel de Plataformas

En concreto, para las Plataformas de gestión de Ciudades Inteligentes, en las que está centrado este Estudio, se proponen las siguientes acciones para reforzar la interoperabilidad:

7. Definir un sitio común y accesible para desarrolladores de la publicación de información sobre APIs y semántica que aplica a cada Plataforma.

8. Además de interoperar con dispositivos y aplicaciones de servicio, se propone el fomento de la federación entre plataformas (interworking), es decir, que las diferentes Plataformas puedan interactuar permitiendo la gestión federada y el intercambio de información.

2. OBJETIVOS DEL DOCUMENTO

El objetivo final es buscar la portabilidad y reutilización de las aplicaciones y la compartición de dispositivos sobre las diferentes Plataformas de Gestión de Ciudades Inteligentes. Este estudio constituye una primera aproximación al conocimiento del concepto de interoperabilidad entre plataformas de gestión de servicios inteligentes. Desde el Plan Nacional de Ciudades Inteligentes está previsto definir estudios que aborden con mayor profundidad los casos de aplicación que se consideren relevantes.

Además se pretende conocer el posible impacto de la estandarización que se está llevando a cabo tanto a nivel nacional, en el CTN 178 de AENOR, como internacional, en el oneM2M, y sus posibles consecuencias en el desarrollo de soluciones Smart Cities en España, y tomar, a partir de las conclusiones de este Estudio, las medidas que se consideren oportunas.

Para ello, el Estudio se ha dividido en las siguientes fases:

- **E1: FASE 1**

  1. **Identificación de puntos de referencia (o confluencia de estándares)** entre los que se puede establecer comparativa entre el modelo de capas propuesto en el documento UNE 178 104 de AENOR [3] y la arquitectura oneM2M [8].

  2. Definición de una **metodología de análisis y cumplimiento de requisitos** para diferentes plataformas comerciales y casos de uso frente a los estándares de referencia.

  3. **Analizar Casos de Uso** reales implantados en diferentes ciudades nacionales conforme establece oneM2M [10]. Los Casos de Uso seleccionados son:

     - Automatización manejo de iluminación en exteriores (calles, etc.)
     - Servicio de compartición de bicicletas
     - Smart Parking
     - Gestión Semafórica
     - Riego inteligente

- **E2: FASE 2**

  Elaboración de **cuestionarios** de cumplimiento de requisitos frente a los estándares de referencia que permitan identificar diferentes grados de compatibilidad con los mismos.

- **E3: FASE 3**

  Propuesta de **soluciones interinas** que pudieran ser utilizadas para asegurar la interoperabilidad de las plataformas seleccionadas, en los casos de uso anteriores, minimizando en lo posible los costes de desarrollo, pero siempre admitiendo, a medio plazo, una evolución hacia los estándares propuestos en oneM2M.

Para completar este Estudio se han generado cuatro documentos, uno introductorio y otros tres correspondientes a cada una de las Fases definidas en el Estudio. Este documento constituye el resultado de la Fase 3 del Estudio.

El objetivo de este documento es proponer soluciones interinas que puedan ser utilizadas para asegurar la interoperabilidad de las plataformas seleccionadas para este Estudio, en los casos de uso analizados en el Anexo del documento o Parte 2, minimizando en lo posible los costes de desarrollo, pero orientado, a medio plazo, una evolución hacia los estándares propuestos en oneM2M.

Se hace especial hincapié en esta fase en las posibilidades de ofrecer portabilidad de aplicaciones a coste razonable, y el potencial que pueden tener los sistemas de adquisición de datos a la hora de compartir mismos dispositivos para diferentes aplicaciones.

3. FASE 3: SOLUCIONES ALTERNATIVAS PARA PLATAFORMAS ANALIZADAS

Las conclusiones más relevantes alcanzadas durante el análisis de casos de uso recogido en el documento o Parte 2 de este Estudio [17][18] son las siguientes:

- El despliegue de los casos de uso incluidos en este Estudio no está integrado de manera masiva a través de las Plataformas en las ciudades españolas.

  Algunas entidades hacen referencia a otros casos de uso si desplegados con las Plataformas de referencia, en la mayor parte de los casos a nivel de piloto, pero no hay muchos despliegues para los Casos de Uso que se plantean en el TR-0001 de oneM2M [8] para Ciudades Inteligentes.

- Respecto a los casos de uso seleccionados y analizados en este Estudio, no hay posibilidad directa de intercambio de sensores y servicios entre las diferentes Plataformas.

  Si se pueden intercambiar, realizando pequeñas adaptaciones, entre aquellas Plataformas que comparten módulos específicos del proyecto FIWARE [1] como el Context Broker o IoTAgents. Para el intercambio con otras Plataformas es necesario realizar algún otro tipo de adaptación, principalmente en el modelo de datos.

Considerando el estado actual de los Casos de uso desplegados y las conclusiones anteriormente reflejadas, existe poca integración real de dispositivos y aplicaciones con las Plataformas de Gestión de Ciudad, por lo que este sería uno de los aspectos a considerar. Para poder cumplir con el objetivo de las Plataformas de Gestión recogidas en la UNE 178 104 [3], es necesario fomentar la integración directa tanto de dispositivos como de aplicaciones o servicios, no a través de otros sistemas que implementan directamente los casos de uso, que en este momento duplican la funcionalidad disponible en las Plataformas.

Como medida transitoria más inmediata se recomienda, para aquellas Plataformas en las que sea posible, incluir elementos del proyecto FIWARE [1] (Context Broker e IoTAgents) u OCEAN [27] que son código abierto y accesible para todo el mundo, con lo que todas la Plataformas ofrecerían un interfaz similar de cara a la interoperabilidad de dispositivos y aplicaciones, hasta que finalmente desarrollen su propio interfaz que cumpla con los estándares nacionales e internacionales (UNE178 104 y oneM2M). Ya hay varias Plataformas de las analizadas en este Estudio que utilizan estos módulos.

Otra medida necesaria es la definición de una semántica común que permita la interoperabilidad semántica. Esta sigue siendo una barrera para la interoperabilidad, no solo a nivel nacional, sino mundial. oneM2M está desarrollando nuevos estándares describiendo más en detalle que semántica común [12] garantiza la interoperabilidad real sin necesidad de desarrollar adaptadores o pasarelas entre los diferentes elementos que componen un ecosistema IoT y como consecuencia de Ciudad Inteligente.

Todas las alternativas recogidas en los apartados siguientes serían también aplicables para alcanzar un mayor grado y garantía de interoperabilidad.

4. FASE 3: SOLUCIONES ALTERNATIVAS GENERALES

Una vez analizados tanto los estándares de referencia como las características actuales de las Plataformas en los Casos de uso para Ciudades Inteligentes del oneM2M y con el objetivo de garantizar la portabilidad de aplicaciones y dispositivos entre diferentes Plataformas de Ciudad se proponen acciones y desarrollos en los siguientes aspectos técnicos:

1. De manera provisional, con el objetivo final de alcanzar el cumplimiento con oneM2M, se considera el desarrollo de nuevos elementos: "**crawlers**" que adapten desde el punto de vista semántico los datos intercambiados entre las Plataformas, los sensores y aplicaciones o **gateways** que hagan de pasarelas adaptando tanto los datos como la conectividad de dispositivos [11], [24], [25].

2. Por otro lado, se estima que el desarrollo y difusión de una **Guía de diseño** que colabore al acercamiento a los estándares tanto de Plataformas como de dispositivos y aplicaciones en la que se defina el desarrollo de nuevas interfaces adaptadas al estándar.

3. Otro paso hacia el aprovechamiento de los desarrollos actuales es potenciar el Interfuncionamiento (interworking) entre Plataformas, para ello será necesario el desarrollos de nuevos elementos, propuestos por el oneM2M [11], llamados **IPE** (Interworking Proxy Entity).

4. Finalmente, el cumplimiento con los estándares oneM2M y la **verificación formal** del mismo por parte de Plataformas, aplicaciones y dispositivos garantizará la convergencia de todos los elementos en un ecosistema abierto, inteligente e interoperable.

Por otro lado, al final de este aparatado también se incluyen otro tipo de medidas que facilitarían la interoperabilidad real entre los elementos que forman parte de la Ciudad Inteligente.

4.1. DESARROLLO DE ELEMENTOS DE ADAPTACIÓN

La mayoría de las soluciones actuales no cumplen, en principio, con los nuevos estándares oneM2M pero están implantadas en diferentes entornos e implementando casos de uso reales.

Aunque el objetivo final es que estas soluciones sigan evolucionando hasta el cumplimiento de los estándares internacionales en el futuro, no se pueden descartar de manera inmediata sino que será necesaria la convivencia de elementos que cumplan los nuevos estándares y otros elementos en uso (plataformas, sistemas o dispositivos) que pueden ser soluciones propietarias que se han desplegado en el pasado y siguen en funcionamiento. Estos sistemas pueden ser:

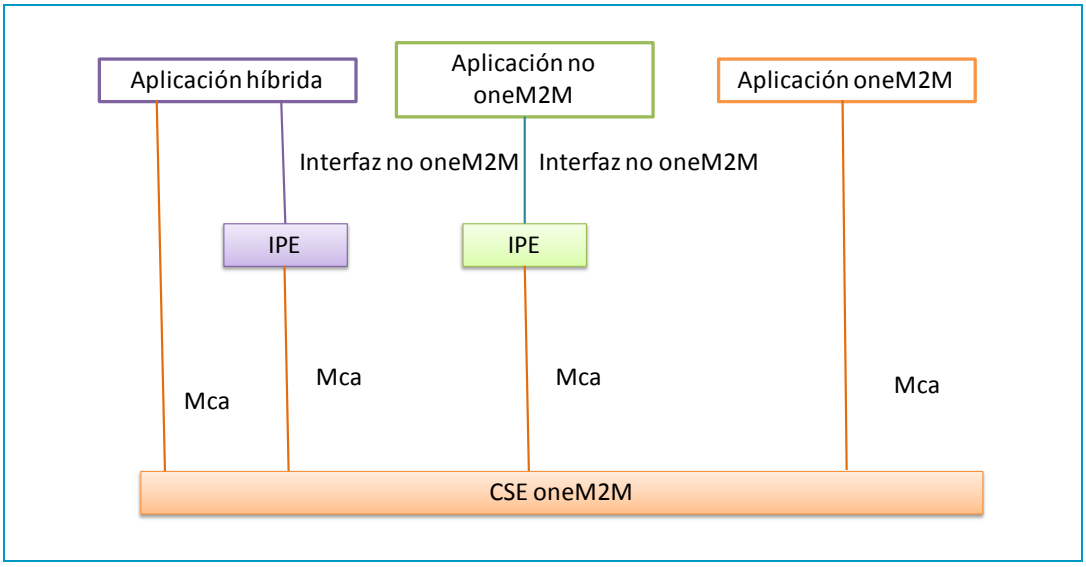
- Despliegues anteriores: a menudo con funcionalidad y modelos de datos propietarios aunque usen interfaces abiertas o estandarizadas para comunicación.

- Nuevas implementaciones pero que siguen prestando servicios de manera vertical y aislada en lugar de aplicar la optimización de los aspectos horizontales.
- Despliegues de red IP no optimizados para oneM2M.

oneM2M está trabajando en la especificación de elementos de adaptación que sirvan para permitir el interfuncionamiento y las arquitecturas mixtas entre elementos no oneM2M con otros que cumplan con los estándares que promueven [11]. En dicho documento, aun en borrador (TS-0014)[11], llaman a dicho elemento de adaptación "Interworking Proxy application Entities (IPE)". Este elemento se caracteriza por hacer de interfaz entre un sistema no oneM2M y realizar una reasignación del modelo de datos ofreciéndolas ya en formato oneM2M a través de las interfaces propias del sistema oneM2M, en este caso a través de la interfaz Mca.

Por lo general se realiza una traducción completa de la semántica del modelo de datos utilizado por el sistema no oneM2M y la lógica de protocolo de interfuncionamiento. Dependiendo de la complejidad del modelo de datos original, pueden darse dos casos: que sea necesaria la definición de un conjunto complejo de recursos construidos a través de los recursos básicos oneM2M, o que se realice una correspondencia sencilla y directa de la comunicación a través de contenedores.

A continuación se muestra la arquitectura propuesta:

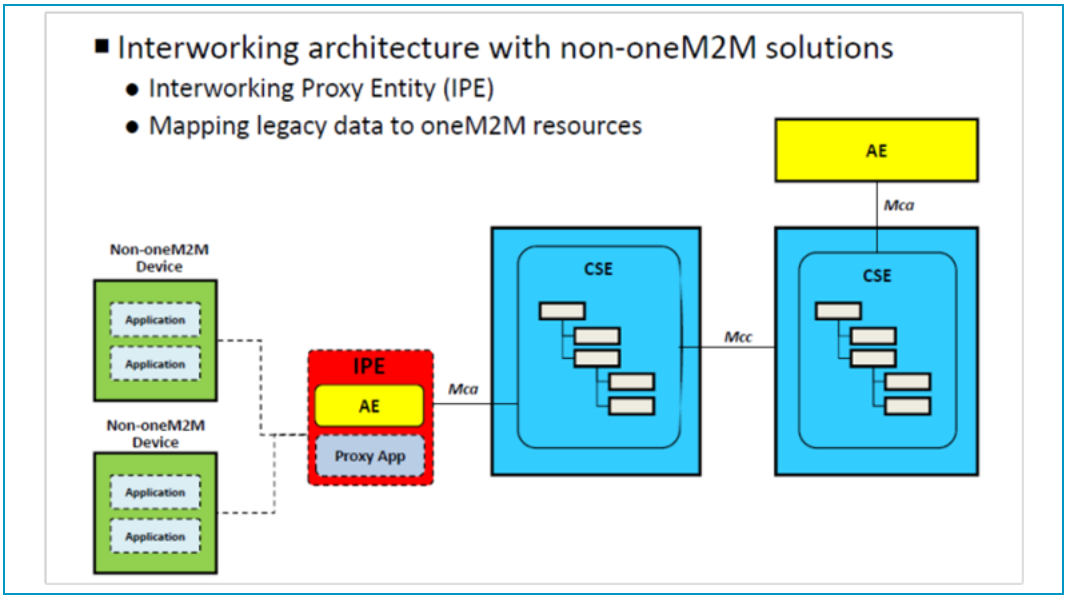


Hay tres formas de conectar con el interfaz Mca a través de un IPE:

- Mapear todo el modelo de datos no oneM2M al modelo de datos oneM2M, basado en contenedores. En este caso el IPE incluye toda la lógica de protocolo de interfuncionamiento.

  Dependiendo de la complejidad del modelo de datos no oneM2M, puede implicar que el IPE construya un complejo conjunto de recursos (a partir de los recursos básicos oneM2M) en el CSE. Estos recursos son representaciones oneM2M del modelo de datos no oneM2M. Permiten el acceso de CSE y AES a las entidades no-oneM2M.

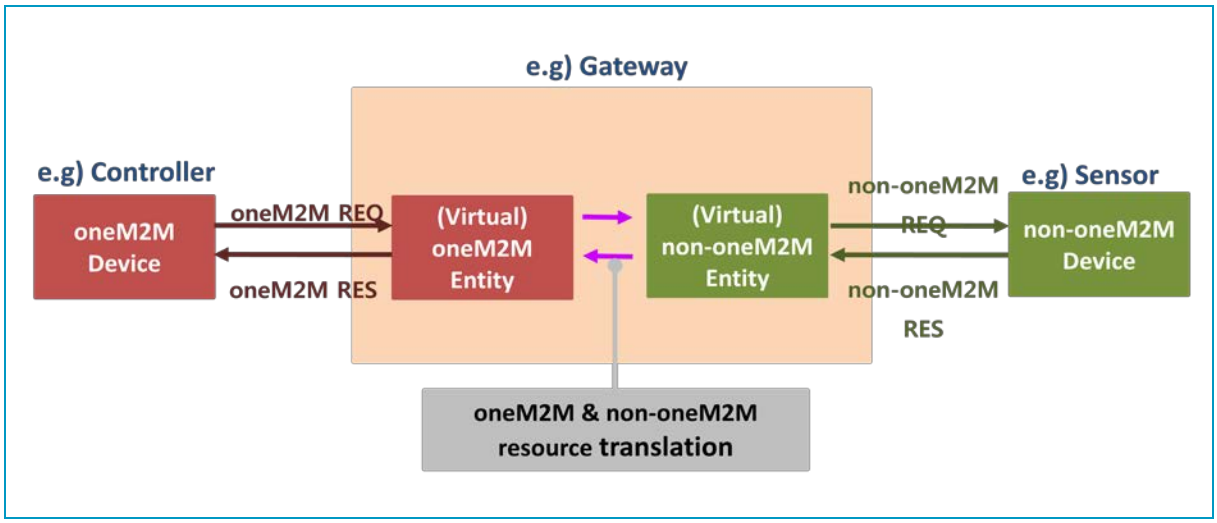
El beneficio de este nivel de interconexión es que ofrece una solución única para permitir las comunicaciones entre diferentes protocolos. El modelo de datos de la solución no oneM2M determina su representación (los nombres, tipos de datos y la estructura de los contenedores) en el sistema M2M. Se atiende a los diferentes niveles de inter-funcionamiento incluyendo protocolo, intercambio de información semántica, intercambio de datos entre las diferentes soluciones y despliegues. Permite ofrecer valores adicionales con respecto a lo que ya está disponible y desplegado a través de protocolos existentes y de servicios de propietarios.



- Utilizar contenedores para el transporte transparente de datos codificados no oneM2M y comandos a través de Mca. Tanto datos como comandos son empaquetados en los contenedores oneM2M. En este caso el CSE o AE necesitan saber las reglas de codificación de protocolo específicas de la solución no oneM2M para poder decodificar el contenido de los contenedores.

- Utilizar mecanismos de reasignación.

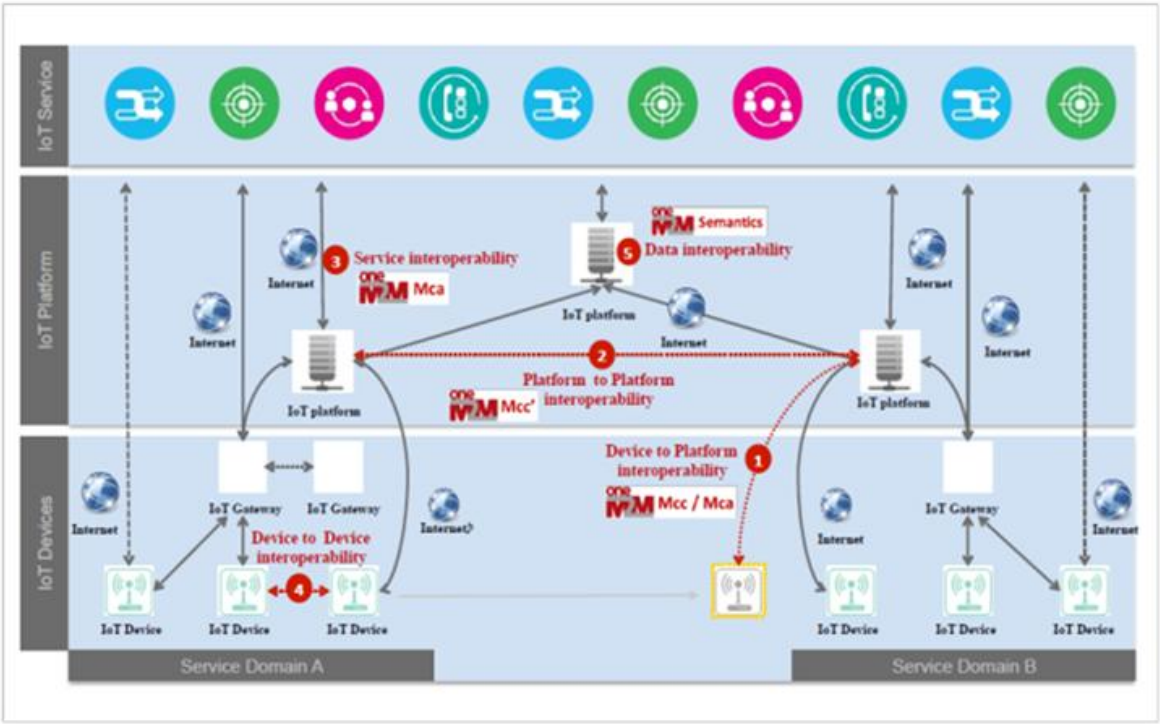
A continuación se muestra un ejemplo de un gateway actuando como IPE entre un sensor no oneM2M con una Plataforma oenM2M.



4.2. DESARROLLO DE NUEVAS INTERFACES. GUÍA DE DISEÑO.

La siguiente propuesta se centra en la modificación, por parte de las Plataformas actuales, de las interfaces de adquisición de datos e interoperabilidad para que cumplan los requisitos oneM2M, incluidas las funcionalidades exigidas en el oneM2M (descubrimiento, localización, registro, gestión de las comunicaciones, etc.).

A continuación se muestra un esquema de las nuevas interfaces que hay que considerar.

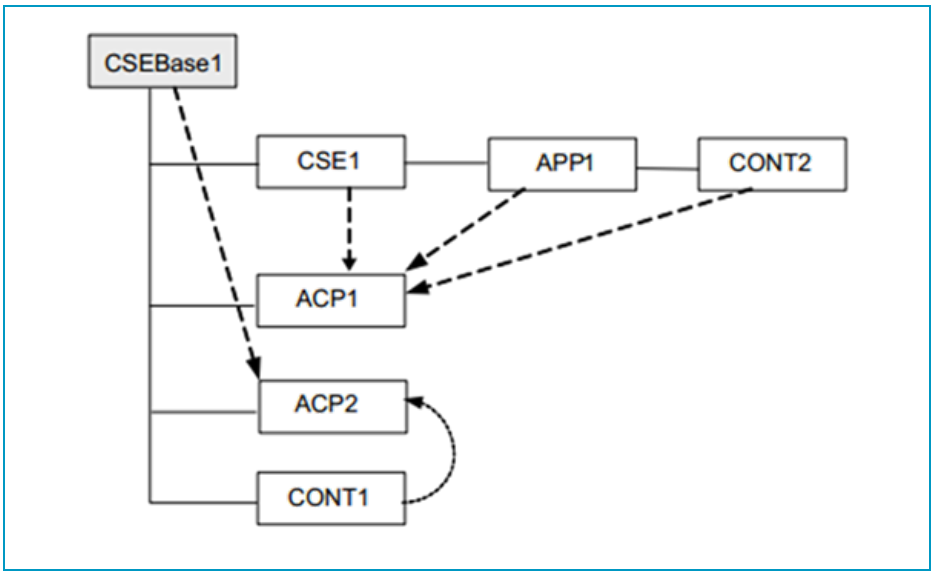


Para estos desarrollos hay que tener en cuenta los siguientes aspectos:

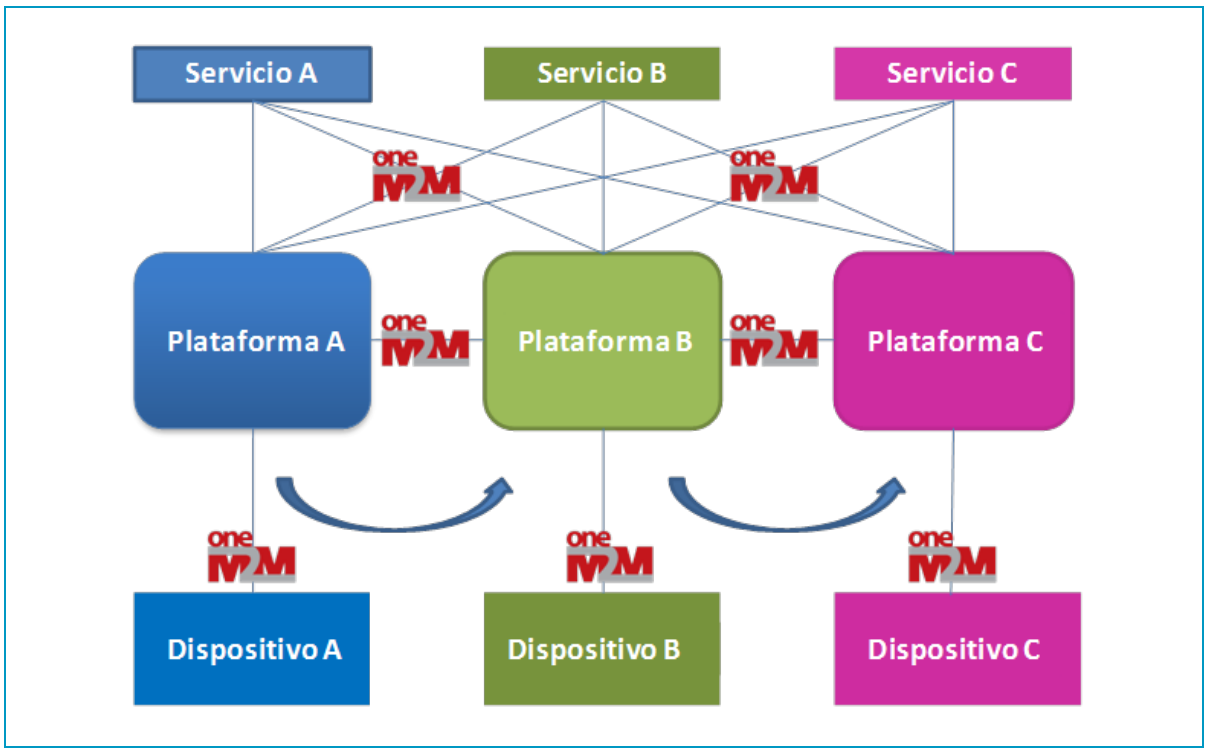
- Deben estar basadas en IP, pero interactuando tecnologías IP y no IP en las redes M2M.
- Deben incluir APIs REST orientadas a recursos, los recursos son representaciones de dispositivos, aplicaciones, cosas y otras descripciones relacionadas, etc.
- Deben tener Inteligencia distribuida entre dispositivos, gateways, cloud, etc.
- Deben poder reutilizar la gestión de dispositivos existentes.
- Deben poder reutilizar los protocolos de intercambio de datos existentes.
- Deben poder reutilizar los mecanismos de seguridad existentes.
- Deben poder reutilizar las capacidades de red subyacentes como la ubicación, los triggers, etc.
- Deben disponer de políticas de control de acceso a los recursos que permitan comunicaciones entre varios.
- Deben estar preparadas para añadir soporte semántico.
- Deben ser independientes respecto a la elección de base de datos, localización de la inteligencia, etc.

Respecto a la definición de recursos basados en el modelo de información

- La información se almacenará en los sistemas como recursos.
- Cada recurso será identificado con un “Uniform Resource Identifier”.
- Cada recurso pertenecerá a un Tipo de recurso tal como se definen en la norma oneM2M
- El Tipo de recurso determina la semántica del recurso
- Los recursos podrán ser creados, leídos, actualizados o borrados
- Los recursos se organizarían en una estructura como se muestra a continuación



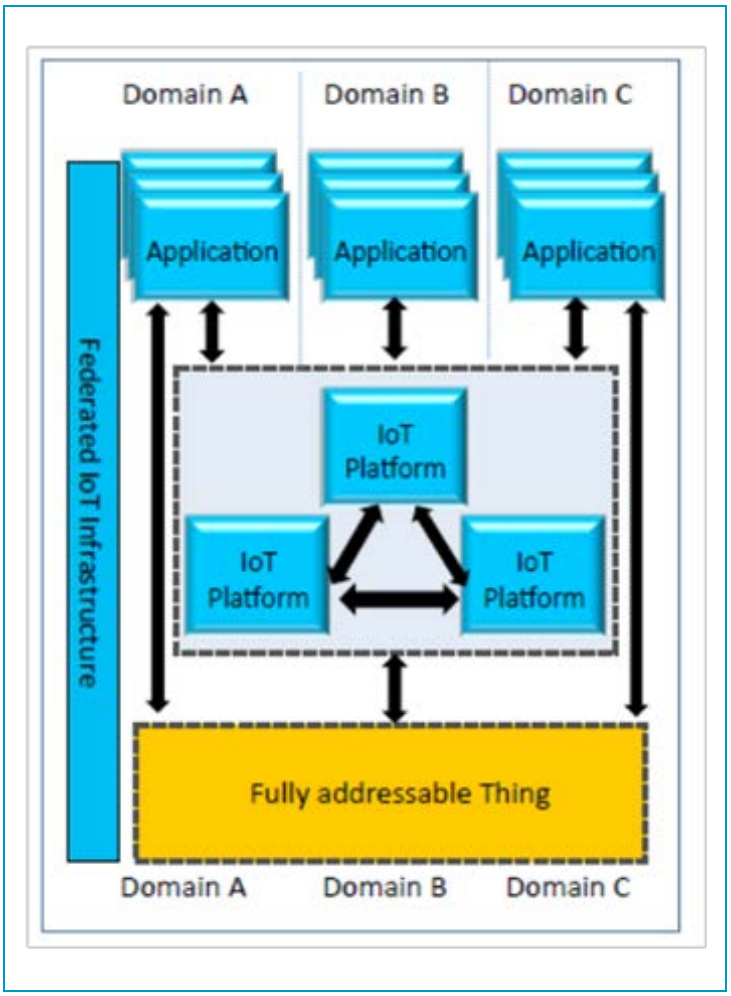
El objetivo final es que tanto servicios, como dispositivos y Plataformas puedan comunicarse todos con todos de manera estandarizada. A continuación se muestra un esquema de cómo sería la comunicación gracias al desarrollo de nuevas interfaces.



oneM2M está desarrollando Guías de diseño de aplicaciones, destinadas a casos de uso concretos, por lo que sería de relevancia darle difusión a la industria nacional de desarrollo de aplicaciones de Ciudades Inteligentes (TR-0025) [14].

4.3. Interoperabilidad entre Plataformas

Aunque en los apartados anteriores se ha considerado la interoperabilidad o interactuación entre diferentes elementos uno de los aspectos más importantes a tener en cuenta de cara a que el ecosistema total de una Ciudad Inteligente sea interoperable es el intercambio de información y la compartición de la gestión entre Plataformas diferentes ya sean conformes a los requisitos oneM2M o no. A este tipo de arquitecturas se las denomina Plataformas Federadas y se muestra a continuación.



Debido a la gran cantidad de servicios y diversas plataformas desplegadas, que cumplen con diferentes estándares o son particulares para ciertos servicios, se hace necesario establecer reglas de convivencia que permitan despliegues más rápidos y mayor aprovechamiento de los recursos en los que ya se han invertido grandes esfuerzos tanto técnicos como económicos.

Para alcanzar estos retos surge el concepto de Arquitecturas de Plataformas Federadas, en las que diferentes plataformas, que pueden estar orientadas a diferentes servicios finales para los ciudadanos, intercambian entres si datos y capacidades de gestión, que estarán distribuidas en diferentes Plataformas pero que serán accesibles desde otras Plataformas diferentes (por ejemplo Plataformas específicas de salud, vehiculares, de gestión de activos de la ciudad, de gestión de servicios o casos de uso de Ciudad Inteligentes, etc.). Con el despliegue de las Plataformas federadas el acceso a los servicios y a los dispositivos serán independientes de las Plataformas a las que están conectadas.

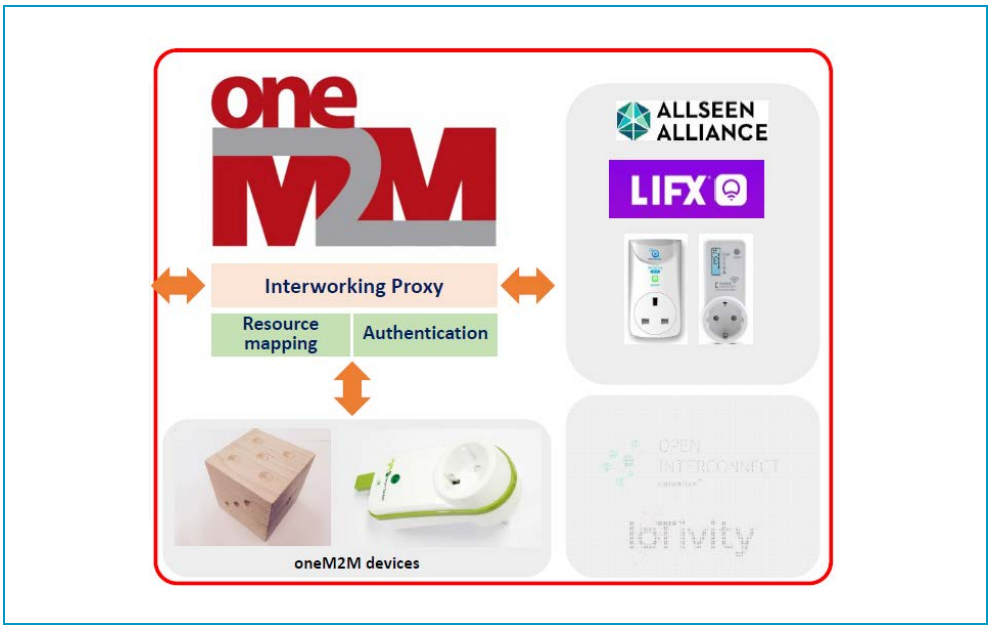
Con este modelo de arquitecturas se consigue:

- Acceder a servicios y funciones de Ciudad Inteligentes desplegados de manera distribuida, de manera que los gastos de despliegue, explotación y mantenimiento pueden ser compartidos por diferentes entidades.
- La convivencia y aprovechamiento de despliegues de servicios desplegados con anterioridad.

- Independencia respecto a servicios y dispositivos

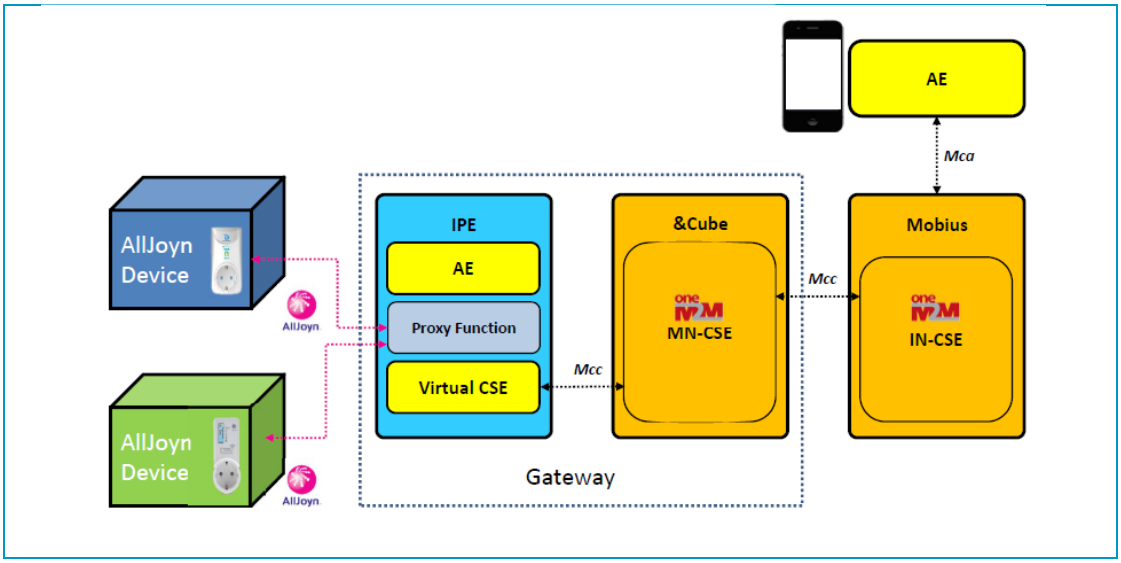
Diferentes Showcases del oneM2M muestran las posibilidades de las Plataformas federadas, tanto para Plataformas oneM2M entre sí con accesos a servicios de Ciudades Inteligentes, como con otras Plataformas no oneM2M y dispositivos no oneM2M [24][25].

A continuación se muestra el ejemplo de interactuación entre una Plataforma oneM2M con dispositivos de la Allseen Alliance (dispositivos AllJoyn) [13].



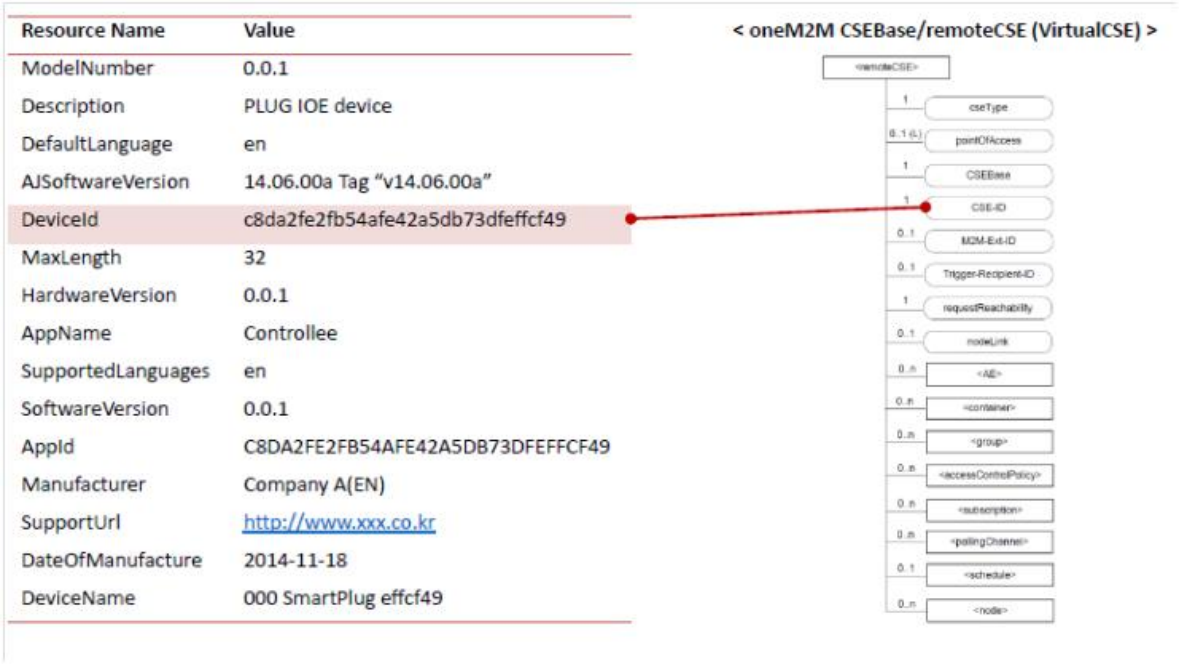
Para alcanzar estos objetivos han desarrollado un IPE con las siguientes características:

- Función Proxy. Es capaz de interactuar con dispositivos AllJoyn
- Mapea una AllJoyn APP como un objeto oneM2M
- Traduce los campos de un mensaje AllJoyn (About) en oneM2M



El mapeo se realiza de la siguiente forma:

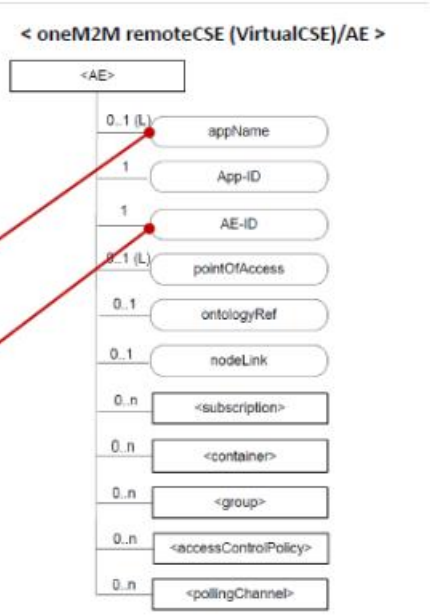
- El identificador del dispositivo AllJoyn se mapea en el CSE-ID



- Otros campos como el modelo, la descripción, la versión, etc., se mapean en los campos oneM2M correspondientes.

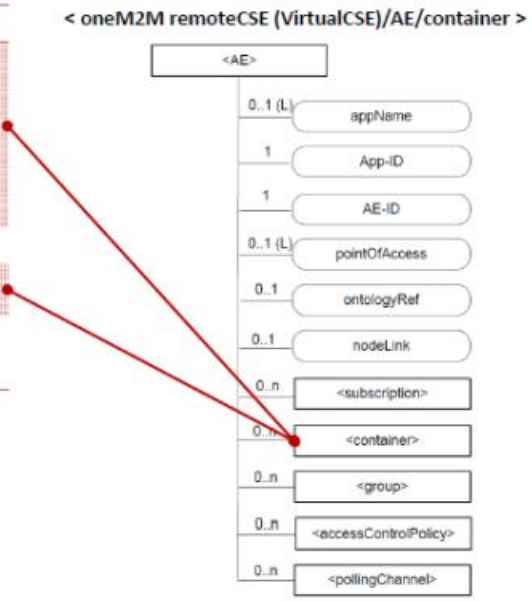
- Igualmente se mapean a el nombre y el identificador de la APP de AllJoyn en oneM2M

Resource Name	Value
ModelNumber	0.0.1
Description	PLUG IOE device
DefaultLanguage	en
AJSoftwareVersion	14.06.00a Tag "v14.06.00a"
DeviceId	c8da2fe2fb54afe42a5db73dfeffcf49
MaxLength	32
HardwareVersion	0.0.1
AppName	Controllee
SupportedLanguages	en
SoftwareVersion	0.0.1
AppId	C8DA2FE2FB54AFE42A5DB73DFEFFCF49
Manufacturer	Company A(EN)
SupportUrl	http://www.xxx.co.kr
DateOfManufacture	2014-11-18
DeviceName	000 SmartPlug effcf49



- Una APP de AllJoyn se mapea en un contenedor oneM2M

Resource Name	Child Resource
Property	Power Status, Power Consumption, Cumulative Power, Volt Value, Current Value, Frequency Value, Power Factor
LabelProperty	-
Action	On, Off
Notification Action	-
Dialog	-



- Como último paso se redireccionan las URI´s de los dispositivos en la Plataforma oneM2M (en este caso Mobius)
  - AllJoyn device URI:
    http://open.iotmobius.com/Mobius/remoteCSEc8da2fe2fb54afe42a5db73dfeffcf49
  - AllJoyn device's AE URI:
    http://open.iotmobius.com/Mobius/remoteCSEc8da2fe2fb54afe42a5db73dfeffcf49/AEC8DA2FE2FB54AFE42A5DB73DFEFFCF49
  - AllJoyn device's container URI:
    http://open.iotmobius.com/Mobius/remoteCSEc8da2fe2fb54afe42a5db7

3dfeffcf49/ AEC8DA2FE2FB54AFE42A5DB73DFEFFCF49/container-PowerStatus

- AllJoyn device's latest PowerStatus retrieval:
  GET
  http://open.iotmobius.com/Mobius/remoteCSEc8da2fe2fb54afe42a5db73dfeff
  cf49/AEC8DA2FE2FB54AFE42A5DB73DFEFFCF49/container/PowerStatus/latest

4.4. CUMPLIMIENTO DE ESTÁNDARES Y CERTIFICACIÓN

La forma más efectiva demostrada de garantizar la interoperabilidad es alcanzar el cumplimiento, por parte de todos los elementos que componen un ecosistema, de los estándares reconocidos a nivel mundial (como es el caso del oneM2M donde han participado la mayoría de los organismos de certificación internacionales como TIA, ETSI, TTA, etc.). Las ventajas que conlleva asegurar el cumplimiento con estos estándares de los diferentes productos pasan por:

- Mejorar la competitividad de las empresas en economías de escala
- Mejorar la oferta y las oportunidades de negocio para los diferentes agentes involucrados
- Simplificar la elección y despliegue de soluciones
- Simplificar los desarrollos teniendo como punto de partida APIs y SDK que cumplen con los estándares
- Disponer de un uso más eficiente y adaptado a las necesidades del servicio de las redes de transporte lo que podrá abaratar el coste de las comunicaciones
- Reducir los ciclos de desarrollo, despliegue y validación de nuevas soluciones que acceden a los mercados internacionales eliminando barreras
- Compartir componentes e infraestructuras por parte de los nuevos servicios de Ciudades Inteligentes
- Mejorar los aspectos de seguridad requeridos en los servicios de la Ciudad Inteligente
- Expandir el uso de los nuevos productos desarrollados a otros Casos de uso relacionados con IoT

Por todos los motivos citados anteriormente, es obviamente recomendable el cumplimiento con los estándares del oneM2M para los nuevos productos y servicios que se desarrollen en España tanto para Ciudades Inteligentes como otras aplicaciones IoT.

Para asegurar que los productos que acceden al mercado cumplen con los estándares es necesario desarrollar un programa formal de certificación de productos frente a estos estándares ya que:

- Proporciona la consistencia en el comportamiento de los dispositivos y servicios compatibles.
- Puede ofrecer una garantía de interoperabilidad entre los dispositivos y servicios de varios fabricantes

- La certificación se otorga a través de un proceso de prueba conforme a las especificaciones y los requisitos oneM2M

Los objetivos a alcanzar por los Programas de Certificación son:

- Mejorar la interoperabilidad
- Acortar el proceso de adopción de productos
- Reducir los costes y el tiempo de adopción de los estándares
- Facilitar la integración de nuevas implementaciones
- Proporcionar confianza en todos los agentes del ecosistema (reguladores, fabricantes, minoristas y consumidores) mediante sellos que garantizan el cumplimiento

Los Programas de Certificación de productos son administrados por Entidades de Certificación y deben contener los siguientes elementos básicos:

- Definición de la política de Certificación y Requisitos
- Definición del Proceso completo de Certificación
- Definición de roles de los Organismos involucrados
- Definición de una metodología de pruebas y el desarrollo de herramientas autorizadas de prueba
- Creación de un logo identificativo y la realización de acciones de difusión del mismo para que sea reconocible por el mercado
- Definición de los requisitos que deban cumplir los laboratorios que validarán las soluciones. Se podrán designar laboratorios independientes en función de la demanda del mercado y la localización de los mismos.

Los grupos de trabajo de oneM2M están desarrollando un Programa de Certificación, pero no se espera que esté operativo al menos hasta final de 2016. Para entonces las empresas españolas deben ir preparándose para cumplir con el proceso de certificación por lo que sería de interés hacer seguimiento de los trabajos que se están realizando y darle difusión en los foros españoles adecuados.

Los resultados de este Estudio, pueden contribuir a ir preparando a la industria nacional a estar listos en el momento de inicio del Programa de Certificación de oneM2M ya que se ha definido una metodología y unas herramientas de medida (cuestionarios) que ayudarán a alcanzar el cumplimiento de los estándares.

4.5. Otras Acciones Recomendadas

Adicionalmente a los aspectos técnicos tratados en los apartados anteriores se enumeran a continuación una serie de acciones que potenciarían alcanzar los objetivos finales de promover la tecnología más adecuada y competitiva dentro de la industria de Tecnologías de la Información y las Comunicaciones nacional.

Acciones a nivel normativo

Por particular relevancia, se detallan aquí recomendaciones concretas en materia de normativa y certificación.

1. En este Estudio se han desarrollado auto-cuestionarios de cumplimiento con las normas UNE 178 104 [3] y oneM2M TS-0001 [8]. Para hacer más fácilmente accesible para todas las empresas interesadas, se propone el desarrollo de una Web donde se puedan completar estos cuestionarios, de manera que la evaluación del grado de cumplimiento se realice automáticamente asignando los resultados para las métricas definidas y de esta manera realizar recomendaciones sobre la hoja de ruta de los productos o acciones específicas según los resultados obtenidos.

2. Uno de los aspectos que pueden ocasionar más problemas a la hora de conseguir la interoperabilidad son los aspectos semánticos. Se recomienda definir un nuevo estándar que recoja claramente un único vocabulario semántico común para todas las Plataformas, dispositivos y apps que se vayan a utilizar en el despliegue de Servicios de las Ciudades Inteligentes en España.

3. Se propone, de cara a acelerar el cumplimiento con los estándares que está promoviendo AENOR en materia de Ciudades Inteligentes, la realización de eventos plugfest para Plataformas y productos Smart Cities (sensores, apps, etc.). Normalmente, estos eventos de interoperabilidad reúnen a diferentes proveedores (a menudo competidores) con el fin de comprobar si sus productos aplican correctamente las normas y son interoperables entre sí. Este enfoque ha demostrado ser una práctica manera de impulsar la interoperabilidad más para el desarrollo de normas, y se ha aplicado con cierto éxito por organizaciones de normalización así como por los consorcios de la industria. Se recomienda un primer evento antes del fin del primer semestre de 2016 y un segundo evento en septiembre-octubre de 2016. Como ejemplo, oneM2M ha organizado uno de estos eventos para la norma TS-0001 en septiembre de 2015 [15], de manera muy satisfactoria, y tiene previsto el próximo evento en mayo de 2016.

4. Realizar Estudios adicionales y de mayor profundidad respecto a casos de uso que tienen mayor despliegue real en las ciudades españolas.

Acciones a Nivel de capacitación del empleo y competitividad

De cara a mejorar el nivel de conocimiento y capacitación de la industria TIC nacional y así aumentar la competitividad se proponen las siguientes acciones:

5. Elaboración de Guías para desarrolladores de productos y servicios de Ciudades inteligentes, proporcionando información y herramientas técnicas para que los desarrollos cumplan con las normas obligatorias (marcado CE, LOPD, etc.) y con los nuevos estándares que van a dar mejoras competitivas a sus productos frente a los mercados nacionales e internacionales.

6. Fomentar la formación y difusión en materia de estandarización, interoperabilidad e industrialización de productos y soluciones de Ciudades Inteligentes tanto para desarrolladores como a la administración pública que actúa como cliente.

Acciones a Nivel de Plataformas

En concreto, para las Plataformas de gestión de Ciudades Inteligentes, en las que está centrado este Estudio, se proponen las siguientes acciones para reforzar la interoperabilidad:

7. Definir un sitio común y accesible para desarrolladores de la publicación de información sobre APIs y semántica que aplica a cada Plataforma.

8. Además de interoperar con dispositivos y aplicaciones de servicio, se propone el fomento de la federación entre plataformas (interworking), es decir, que las diferentes Plataformas puedan interactuar permitiendo la gestión federada y el intercambio de información.

5. ACRÓNIMOS

AE	*Application Entity (oneM2M architecture)*
AEN/CTN	*Comité Técnico de Normalización de AENOR*
API	*Application Programming Interface*
APP	*Application*
ARIB	*Association of Radio Industries and Businesses*
ATIS	*Alliance for Telecommunications Industry Solutions*
CE	*Conformité Européenne*
CSE	*Common Service Entity (oneM2M architecture)*
ETSI	*European Telecommunications Standards Institute*
IPE	*Interworking Proxy Entity*
IoT	*Internet of Things*
LOPD	*Ley Orgánica de Protección de datos*
M2M	*Machine to Machine communications*
Mca	*Interfaz entre un CSE y un AE*
REST	*Representational State Transfer*
SDK	*Software development kit*
SETSI	*Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información*
TIA	*Telecommunications Industry Association (North America)*
TIC	*Tecnologías de la información y la comunicación*
TR	*Technical report*
TS	*Technical specification*
TTA	*Telecommunications Technology Association (Korea)*
TTC	*Elecommunication Technology Committee (Japan)*
UNE	*Una Norma Española*
URI	*Uniform Resource Identifier*
WSN	*Wireless sensor network*

6. REFERENCIAS

[1] https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/File:Fiware-citymap.jpg

[2] http://www.agendadigital.gob.es/planesactuaciones/Bibliotecaciudadesinteligentes/2.Materialcomplementario/normas_ciudades_inteligentes.pdf

[3] UNE 178 104 Ciudades Inteligentes (AENOR). Infraestructuras. "Sistemas integrales de gestión de la Ciudad Inteligente"

[4] UNE 178 301 (AENOR). "Ciudades Inteligentes. Datos abiertos"

[5] UNE 178 107-4 (AENOR) Guía para las infraestructuras de Ciudades Inteligentes. Redes de acceso y transporte. Parte 4: Redes de Sensores, WSN

[6] UNE 178 102-X (AENOR) Ciudades Inteligentes. Infraestructuras. Sistemas de telecomunicación

[7] PNE 178 4XX- Borradores de norma del grupo de trabajo GT4 de AENOR

[8] TS-0001 (oneM2M). "Functional Architecture". V1.6.1

[9] TS-0002 (oneM2M). "Requirements" V1.0.1

[10] TR-0001 (oneM2M). "oneM2M Use Cases Collection" V0.0.5

[11] TS-0014 (oneM2M). "LWM2M Interworking". Borrador.

[12] TS-0012 Bse Ontology. Borrador

[13] TS-0021 oneM2M and AllJoyn interworking. Borrador

[14] TR-0025 Application developper Guide. Borrador.

[15] Interop Test Event Report 1.1.0. oneM2M. (2015-10)

[16] Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes. Red.es. PARTE 1: Introducción.

[17] Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes. Red.es. PARTE 2: Metodología.

[18] Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes. Red.es. PARTE 2: Metodología. ANEXO confidencial.

[19] Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes. Red.es. PARTE 3: Cuestionarios

[20] http://www.agendadigital.gob.es/planes-actuaciones/Bibliotecaciudadesinteligentes/2.Materialcomplementario/normas_ciudades_inteligentes.pdf

[21] http://www.agendadigital.gob.es/planes-actuaciones/Paginas/plan-nacional-ciudades-inteligentes.aspx

[22] https://allseenalliance.org/

[23] https://allseenalliance.org/framework

[24] Interoperability Test Based on Opensource IoT Platforms. Korea Electronics Technology Institute

[25] oneM2M. Showcase C:Smart City Services and Multiple Service Layer Platforms InterworkingInteroperability Test Based on Opensource IoT Platforms

[26] Proyecto Europeo VITAL: Virtualized programmable InTerfAces for innovative cost-effective IoT depLoyments in smart cities

[27] http://www.iotocean.org