DIPUTACIÓN DE BADAJOZ

Desarrollo de la iniciativa "Plataforma Provincial de Gestión Inteligente de Servicios Públicos"

Integración con la Plataforma Provincial de Gestión Inteligente de Servicios Públicos de la Diputación de Badajoz

22/05/2018

Índice

1 Control de cambios del documento

Versión	Fecha	Responsable	Modificaciones
V01.0	22/05/18	RGD	Creación documento
V02.0	06/08/19	RGD	Añadidos nuevos comentarios
V03.0	05/06/20	RGD y AHMO	Añadidos nuevos comentarios
Versión Final			

2 Introducción

El objeto de este documento es detallar los requisitos de integración con la Plataforma Provincial de Gestión Inteligente de Servicios Públicos de la Diputación de Badajoz, indicando las distintas posibilidades de interoperabilidad, las características de la Plataforma Provincial y el modelo de relación e integración de los datos con la misma en cada caso.

3 Integración con la Plataforma Provincial de Gestión Inteligente de Servicios Públicos de la Diputación de Badajoz

La arquitectura de cada servicio debe constar de 3 componentes: Software de Gestión de un servicio o ASV (Application Server Vertical), la Plataforma de Gestión Inteligente de Servicios Públicos y los dispositivos de captación de información IoT y/o Servidor de Aplicaciones externo EAS (External Application Server).

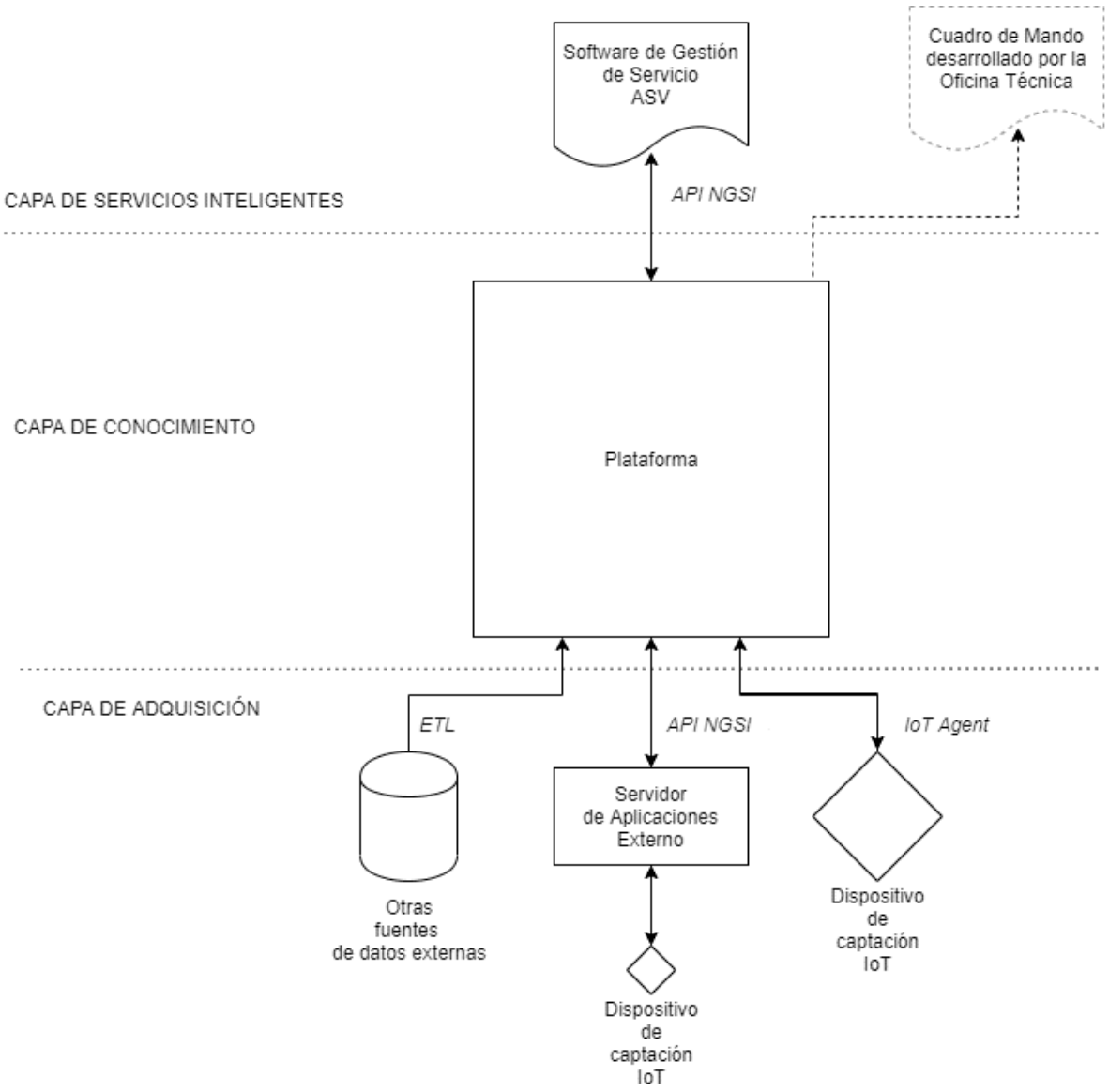
El Software de Gestión de un Servicio (ASV) se encargará de visualizar la información operacional, gestionar el estado de los dispositivos, etc. Se permite la recepción de información operacional y/o de mantenimiento directamente desde los propios Dispositivos al Software de Gestión de un Servicio (ASV).

La Plataforma de Gestión Inteligente de Servicios Públicos será el eje centralizador de la información.

El Servidor de Aplicaciones Externo EAS será el encargado de aportar la capa de inteligencia para recoger la información de los Dispositivos y enviarlo a la Plataforma en el formato adecuado, siendo este esquema de trabajo recomendable solo en caso de que los Dispositivos de captación IoT no posean la suficiente inteligencia para realizarlo por sí mismos.

Los Dispositivos de captación IoT son los sensores que obtienen y remiten la información.

Se considera Otras fuentes de datos externas cualquier fuente de información que no proviene de un Dispositivo de captación IoT, como por ejemplo un aplicativo tipo Chatbot o una Base de datos.



El modelo objetivo pretende independizar el software de gestión de un servicio ASVs (que tradicionalmente es el componente que visualiza la información más operativa) de los dispositivos de captación de información IoT y/o Servidor de Aplicaciones externo.

En este nuevo modelo objetivo, los ASVs deberán tener la posibilidad de operar de forma bidireccional con los dispositivos de captación de información y/o Servidor de Aplicaciones externo a través de la Plataforma. Para conseguirlo, cada software de gestión de un servicio ASV debería incluir, además de sus propios apartados de funcionalidades particulares específicas de gestión y control de esa vertical, los desarrollos y/o servicios correspondientes integrados en la Plataforma para llevar a cabo esta comunicación bidireccional y poder proporcionar la funcionalidad correspondiente al servicio a prestar.

La Plataforma siempre deberá ser fuente de recepción de los datos de los dispositivos de captación de información IoT, de los Servidores de Aplicaciones Externo o de Otras fuentes de datos externas. La información será enviada a la Plataforma, en todo caso, siguiendo el estándar de modelado FIWARE (https://www.fiware.org/developers/data-models/).

Desde la Plataforma se debe recoger la información por parte de los ASVs a través de las API / SDKs que proporciona la Plataforma para su visualización.

Nota: Aunque no sea el esquema más recomendable, se permite que los dispositivos de captación de información IoT, el Servidor de Aplicaciones Externo y/o Otras fuentes de datos externas envíen información a su Software de Gestión de Servicio (ASV) de tipo operativo y mantenimiento de forma directa. Este esquema de trabajo no exime al proveedor de realizar el envío de la información que se solicite a la Plataforma.

Con respecto a la conectividad entre los dispositivos de captación de información IoT , Servidor de Aplicaciones externo y/o Otras fuentes de datos externas con la Plataforma, la Plataforma cuenta con una capa de Adquisición en la que existen los siguientes tipos de integraciones:

3.1 Integración de sensores o elementos de campo (IoT Agents)

Dentro de este apartado, pueden encontrarse tres tipos de integraciones con la Plataforma:

3.1.1 Integración de elementos de campo nativos en alguno de los protocolos de comunicación disponibles en la Plataforma de forma preferentemente bidireccionals

Este caso es aplicable cuando existe la posibilidad de un despliegue de los elementos de campo compatibles con los protocolos de transporte ya disponibles en la Plataforma (MQTT, HTTP) así como con sus modelos de datos (UL2.0, JSON, LWM2M).

Cada uno de los protocolos IoT podrá emplearse usando los distintos protocolos de transporte dando lugar a las siguientes parejas de protocolos de intercambio de información. Los protocolos más habituales son:

- HTTP – JSON, HTTP – UL2.0
- MQTT – UL2.0
- HTTP - LWM2M

Se puede consultar la lista, no exhaustiva, de fabricantes y dispositivos en el programa **FIWARE IoT Ready** (https://marketplace.fiware.org/). Aunque un posible partner no esté inicialmente certificado en FIWARE IoT Ready para interactuar con la Plataforma Badajoz es Más, puede certificarse, ya que el proceso desarrollado para ello es lo suficientemente flexible y fácil de usar para garantizar una integración de un nuevo tipo de elemento de campo.

Las órdenes y comandos de los IoT Agents sólo pueden funcionar en aquellos entornos en los que la comunicación con los dispositivos es bidireccional. Si no es posible implantar una solución bidireccional, serán válidas soluciones unidireccionales.

En caso de dispositivos fácilmente programables (PoC, SmartDevices, etc.) se recomienda su adaptación a alguno de los estándares soportados por la Plataforma Badajoz es Más.

3.1.2 Integración de elementos de campo no nativos

El segundo caso es aplicable ante dispositivos ya desplegados o con fabricantes no certificados.

Se resuelve mediante la creación de agentes/gateways/conectores integrados a medida o bien mediante la instalación remota de un agente software directamente en el elemento de campo, el cual realiza la conversión de protocolos y formatos al estándar NGSI.

La creación de los agentes/gateways/conectores puede realizarse por cualquier actor de la cadena de valor: fabricante del elemento de campo, integrador, etc. puesto que el SDK de creación de IoT Agents es abierto y disponible como herramienta de uso externo. (FIWARE IOT AGENT FRAMEWORK https://iotagent-node-lib.readthedocs.io/en/latest/).

3.1.3 Integración de elementos de campo no nativos y accesibles desde un backend propietario

La tercera opción se refiere a aquellos elementos de campo cuya comunicación se realiza siempre a través de un sistema de backend propietario, es decir, un Servidor de Aplicaciones Externas.

Para aquellos sistemas backend que de forma nativa no soporten el estándar NGSI es necesario crear el adaptador correspondiente (Context Adapter), que corresponderá generalmente con un módulo de comunicación, una ETL o un Middleware.

El desarrollo e implantación de esta solución será llevada a cabo por el proveedor de los datos de cada componente y / o la Oficina Técnica. Siempre deberá utilizar las llamadas API REST NGSI de la Plataforma para el envío de los datos a la Plataforma Badajoz es Más.

En caso de que el proveedor de los datos aloje su sistema backend en un servidor externo a la Diputación de Badajoz deberá disponer de una IP / dominio fijo a fin de facilitar la integración con la red de la Diputación de Badajoz.

3.2 ETL

Los datos son extraídos directamente de la solución software del proveedor y/o de los sistemas de gestión municipal o legacy, y son transformados para su integración.

El desarrollo e implantación de dicha transformación se realizará en formato ETL y será llevada a cabo por parte de la Oficina Técnica de la Diputación de Badajoz y/o la empresa proveedora en función de la magnitud de la solución a desarrollar.

En caso de que el proveedor de los datos aloje la solución ETL en un servidor externo a la Diputación de Badajoz, deberá disponer de una IP / dominio fijo a fin de facilitar la integración con la red de la Diputación de Badajoz.

4 API NGSI de integración con la Plataforma Provincial de Gestión Inteligente de Servicios Públicos

Una vez seleccionado el método de integración, y con el objetivo de obtener una certificación FIWARE que permita la interoperabilidad con la Plataforma Provincial, será necesario utilizar las llamadas proporcionadas por la API NGSI REST que puede descargar de aquí:

https://www.getpostman.com/collections/d309ce22078eb96cf4c8

Esta API contiene un conjunto de operaciones básicas para utilizar con la Plataforma, divididas en las siguientes categorías:

- *IDM & Auth*: Seguridad de Plataforma, petición de tokens
- *Orion Context Broker*: Gestión de entidades, atributos y subscripciones
- *IOTA*: Gestión de dispositivo IoT y envío de medidas desde sensores
- *STH*: Almacenamiento de tiempo corto
- *Perseo CEP*: Gestión de reglas de alarmado
- *CKAN*: Gestión de datos para envío a Portal de Datos Abiertos

La Oficina Técnica del Proyecto Badajoz es Más generará los siguientes recursos:

- Subservicio en el entorno en el que se vayan a integrar los datos además del usuario y contraseña particular
- Modelo de Datos teórico en base a los datos proporcionados y la Base de datos que la albergará
- Valoración de la forma de interconexión óptima para el tipo de datos indicado.
- Documentación de integración con IPs y puertos

En función de este tipo de interconexión, se contemplan dos opciones:

4.1 Integración con elementos de campo nativos

Se llevará a cabo una integración por IoT Agent mediante HTTP. Los datos podrán enviarse en formato JSON o UL..

Los pasos serán los siguientes:

1º Debe implementar la seguridad requerida

La seguridad estará implementada al incluir en la llamada para el envío de datos el API Key proporcionado por el equipo del proyecto "Badajoz Es Más" {{Device_APIkey}}. Existirá una API Key por cada entidad a integrar.

2º Realizará el envío de datos mediante el método indicado y que tiene desarrollada la implementación de la seguridad realizada en el paso anterior

Se utilizarán las llamadas contenidas en la carpeta IOTA.

El envío de los datos se realizará mediante la siguiente llamada POST HTTP:

```
http://{{{ENDPOINT}}}:{{{PORT}}}/iot/json?
k={{{Device_APIkey}}}&i={{{myEntity}}}&getCmd=0
```

En "Headers" se debe indicar:

```
Content-Type: application/json
```

y en el body del código por otro lado debe ir el código JSON.

3º Comprobará que los datos están entrando correctamente a la Plataforma mediante las llamadas a la API de la Plataforma Provincial indicadas

Se utilizarán las llamadas contenidas en la carpeta Orion Context Broker.

Comprobar todas las entidades: Mediante una llamada GET podemos consultar el total de entidades creadas:

```
http://{{{ENDPOINT}}}:{{{PORT}}}/v2/entities
```

En “Headers” se debe indicar:

```
Fiware-Service: {{service}}
Fiware-ServicePath: {{subservice}}
```

X-Auth-Token: (Token generado cada 30 minutos aproximadamente)

Comprobar una entidad individual: Podemos también mediante GET obtener los datos de una entidad individualmente:

```
http://{{{ENDPOINT}}}:{{{PORT}}}/v2/entities/{{myEntity}}
```

Donde {{myEntity}} es la entidad a consultar.

En “Headers” se debe indicar:

```
Fiware-Service: {{service}}
Fiware-ServicePath: {{subservice}}
```

X-Auth-Token: (Token generado cada 30 minutos aproximadamente)

En caso de errores, puede utilizar las siguientes llamadas:

Borrar Entidades: Llamada DEL siguiente:

```
http://{{{ENDPOINT}}}:{{{PORT}}}/v2/entities/{{myEntity}}
```

Donde {{myEntity}} es la entidad a borrar.

En “Headers” se debe indicar:

`Fiware-Service: {{service}}`

`Fiware-ServicePath: {{subservice}}`

`X-Auth-Token:` (Token generado cada 30 minutos aproximadamente)

Borrar atributos: Es una llamada DEL y sería la siguiente:

```
http://{{{ENDPOINT}}}:{{{PORT}}}/v2/entities/{{myEntity}}/attrs/
{{attribute}}
```

Donde {{myEntity}} es la entidad a la que queremos borrar el atributo y attribute es el atributo a borrar.

En “Headers” se debe indicar:

`Fiware-Service: {{service}}`

`Fiware-ServicePath: {{subservice}}`

`X-Auth-Token:` (Token generado cada 30 minutos aproximadamente)

La empresa proveedora debe asegurarse de que las entidades y atributos se generan correctamente y los datos que se envíen sean los correctos, así como la actualización / borrado / añadido de entidades y atributos dentro de su subservicio. La empresa proveedora realizará la integración en los entornos DEV, PRE y PRO de la Plataforma.

4.2 Integración con elementos de campo no nativos

Se llevará a cabo una integración directa contra Context Broker usando la API NGSI mediante HTTP. Los datos podrán enviarse en formato JSON o UL.

Los pasos serán los siguientes:

1º Debe implementar la seguridad requerida

Para ello deberá utilizar las llamadas incluidas en la carpeta IDM & Auth.

A continuación, se muestra un ejemplo de llamada POST de petición de token a la Plataforma.

```
http://{{{ENDPOINT}}}:{{{PORT}}}/v3/auth/tokens
```

Body:

```
{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "domain": {
                        "name": "{{service}}"
                    },
                    "name": "{{user}}",
                    "password": "{{password}}"
                }
            }
        },
        "scope": {
            "project": {
                "domain": {
                    "name": "{{service}}"
                },
                "name": "{{subservice}}"
            }
```

```
        }
    }
}
```

y en “Headers” se indica:

```
Content-Type: application/json
```

El token debe renovarse cada 30 minutos aproximadamente.

2º Realizará el envío de datos mediante el método indicado y que tiene desarrollada la implementación de la seguridad realizada en el paso anterior

El envío de datos se seguirá utilizando el modelo FIWARE acordado con la Oficina Técnica. Se utilizarán las llamadas contenidas en la carpeta Orion Context Broker.

Un ejemplo de llamada POST para crear cada entidad es la siguiente:

```
http://{{{ENDPOINT}}}:{{{PORT}}}/v2/entities
```

En “Headers” se debe indicar:

```
Fiware-Service: {{service}}
Fiware-ServicePath: {{subservice}}
X-Auth-Token: (Token generado cada 30 minutos aproximadamente)
Content-Type: application/json
```

y en el Body del código debe ir el código JSON.

Puede utilizar la misma llamada POST anterior para actualizar los atributos de la entidad creada.

3º Comprobará que los datos están entrando correctamente a la Plataforma mediante las llamadas a la API de la Plataforma Provincial indicadas

Se utilizarán las llamadas contenidas en la carpeta Orion Context Broker.

Comprobar todas las entidades: Mediante una llamada GET podemos consultar el total de entidades creadas:

```
http://{{{ENDPOINT}}}:{{{PORT}}}/v2/entities
```

En “Headers” se debe indicar:

```
Fiware-Service: {{service}}
Fiware-ServicePath: {{subservice}}
X-Auth-Token: (Token generado cada 30 minutos aproximadamente)
```

Comprobar una entidad individual: Podemos también mediante GET obtener los datos de una entidad individualmente:

```
http://{{{ENDPOINT}}}:{{{PORT}}}/v2/entities/{{myEntity}}
```

Donde {{myEntity}} es la entidad a consultar.

En “Headers” se debe indicar:

```
Fiware-Service: {{service}}
Fiware-ServicePath: {{subservice}}
X-Auth-Token: (Token generado cada 30 minutos aproximadamente)
```

En caso de errores, puede utilizar las siguientes llamadas:

Borrar Entidades: Llamada DEL siguiente:

```
http://{{{ENDPOINT}}}:{{{PORT}}}/v2/entities/{{myEntity}}
```

Donde {{myEntity}} es la entidad a borrar.

En “Headers” se debe indicar:

```
Fiware-Service: {{service}}
Fiware-ServicePath: {{subservice}}
X-Auth-Token: (Token generado cada 30 minutos aproximadamente)
```

Borrar atributos: Es una llamada DEL y sería la siguiente:

```
http://{{{ENDPOINT}}}:{{{PORT}}}/v2/entities/{{myEntity}}/attrs/
{{attribute}}
```

Donde {{myEntity}} es la entidad a la que queremos borrar el atributo y attribute es el atributo a borrar.

En “Headers” se debe indicar:

```
Fiware-Service: {{service}}
Fiware-ServicePath: {{subservice}}
X-Auth-Token: (Token generado cada 30 minutos aproximadamente)
```

La empresa proveedora debe asegurarse de que las entidades y atributos se generan correctamente y los datos que se envíen sean los correctos, así como la actualización / borrado / añadido de entidades y atributos dentro de su subservicio.

La empresa proveedora realizará la integración en los entornos DEV, PRE y PRO de la Plataforma.

5 Referencias

- FIWARE CONTEXT BROKER (Orion)

https://fiware-orion.readthedocs.io/en/master/

- FIWARE Datamodels

https://www.fiware.org/developers/data-models/

- FIWARE Thinking Cities Postman Collection

https://www.getpostman.com/collections/d309ce22078eb96cf4c8