Cazadores de mitos en la DGT 3.0

Análisis técnico, ecosistema, protocolos y ciberseguridad de la señal V16

Pedro C. aka “s4ur0n” (@NN2ed_s4ur0n)

/Rooted



Cazadores de mitos en la DGT 3.0

Análisis técnico, ecosistema, protocolos y ciberseguridad de la señal V16

Pedro C. aka “s4ur0n” (@NN2ed_s4ur0n)

Whoami

/Rooted



```
class PedroC:
    def __init__(self):
        self.name = 'Pedro Candel’
        self.nick = 's4ur0n'
        self.rrss = '@NN2ed_s4ur0n'
        self.email = 's4ur0n@s4ur0n.com'
        self.web = 'https://www.s4ur0n.com'
        self.company = 'CS3 Group'
        self.corpweb = 'https://cs3group.com'
        self.role = 'Security Researcher'
        self.work = ['Offensive Security', 'Auditor', 'Rev']
        self.group = ['OWASP', 'mlw.re’, '...']
        self.hobby = ['Fly', 'Sail', 'Ski', 'BBQs', '...']
        self.hate = ['SmokeSellers', 'Pr0nStars']
```

CS3 SECURITY SERVICES https://cs3group.com

OWASP Open Web Application Security Project

mlw.re hunting Malware like a sir

Disclaimer

/Rooted

El autor **no tiene ningún tipo de vinculación** con las empresas fabricantes, terceras, distribuidores, DGT, Gobierno de España o el Ministerio del Interior con respecto a la investigación llevada a cabo.

Tampoco es partidario de ellas como dispositivo primario de señalización, por su inseguridad demostrada bajo ciertas condiciones, aunque para la exposición, nos centraremos en otros aspectos técnicos como su documentación, APIs y su ***ciberseguridad*** sin entrar a valorar otras cuestiones.



Contenido

- Ecosistema de IoT
- Acceso a la documentación técnica
- Legislación aplicable
- Protocolos y mensajes de la señal V16
- API Rest para el envío de eventos
- Señal V16: funcionamiento
- Señal V16: componentes hardware
- Señal V16: ataques
- Reversing
- Explotación de los datos recopilados
- Conclusiones




GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
DGT
Dirección General de Tráfico
/Rooted
Plataforma DGT 3.0
Ecosistema de IoT
V16
CONECTADA
A DGT 3.0
Obligatoria desde
01/01/26
Dispositivo que aumenta tu seguridad.
Para vehículos inmovilizados en carretera.

Plataforma DGT 3.0

La plataforma de la **DGT 3.0 para IoT**, ha sido desarrollada en la nube pública, con capacidades de ***escalabilidad***, ***disponibilidad***, ***seguridad*** y ***portabilidad***, que permite la interconexión entre todos los actores que forman parte del ecosistema de tráfico y movilidad.

Está diseñada para comunicarse con los backends de cada uno de los distintos actores donde estarán alojadas las **aplicaciones servidor**, que ***comparten y/o consumen*** la información.





Plataforma DGT 3.0

Estas aplicaciones servidor se conectarán a su vez a la **aplicación Cliente** de cada uno de los actores que podrá estar alojada en: balizas, dispositivo móvil, vehículos, etc; y con la ***funcionalidad que corresponda*** según el tipo de actor (comparte o consume información).

Los métodos utilizados para compartir y consumir información con la plataforma DGT 3.0 están **basados en los estándares** de mercado ***API REST*** y ***colas MQTT***, según el caso de uso que se quiera implantar.

Plataforma DGT 3.0

Para poder **acceder a DGT 3.0**, es requisito:

- Cumplimentar previamente el cuestionario en https://dgt1.typeform.com/to/G6kzdafw?typeform-source=www.dgt.es
- Una **IP pública de su backend en la lista blanca** (Whitelist) de la plataforma DGT 3.0
- Un **Certificado Digital x.509 v3 de cliente** para la ***autenticación*** y ***autorización*** de las comunicaciones, que será emitido por una Autoridad de Certificación (CA) interna de la plataforma DGT 3.0


GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
DGT
Dirección General de Tráfico
/Rooted
Plataforma DGT 3.0
Acceso a la documentación técnica
V16
CONECTADA A DGT 3.0
Obligatoria desde
01/01/26
Dispositivo que aumenta tu seguridad.
Para vehículos inmovilizados en carretera.

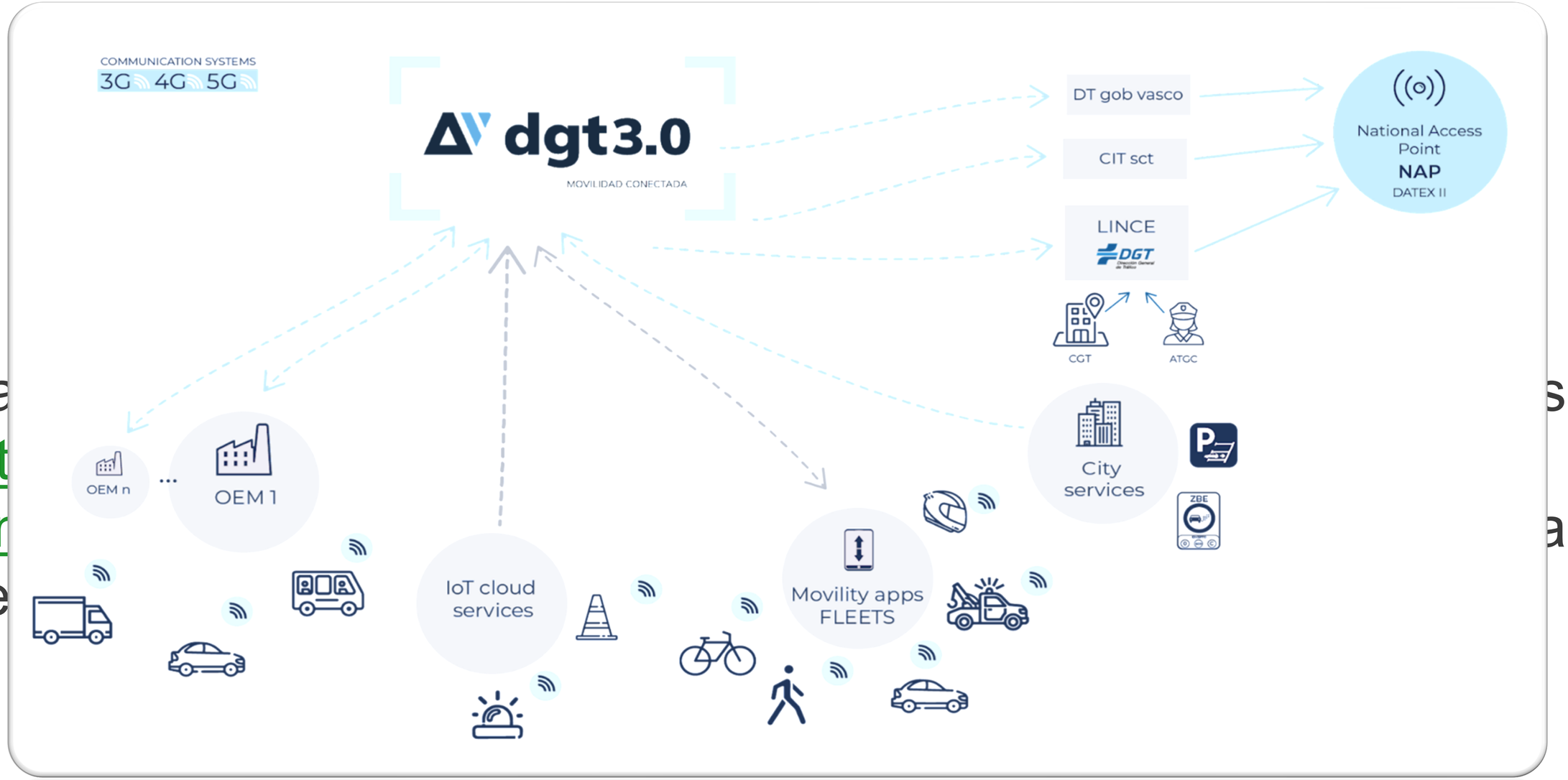
Acceso a la documentación técnica

/Rooted

De forma ***pública*** y ***sin necesidad de estar registrado*** en la plataforma, se dispone actualmente de **toda la documentación técnica** para los datos de:

- ✓ Advertencia Averías en Carretera (V16)
- ✓ Zonas de Bajas Emisiones (ZBE)
- ✓ Seguimiento de Vehículos Especiales (V2)
- ✓ Ubicación de Grúas de auxilio en carretera en operación.
- ✓ Eventos Deportivos.
- ✓ Aparcamientos.
- ✓ Protección de Operarios trabajando Vías (Cono conectado)

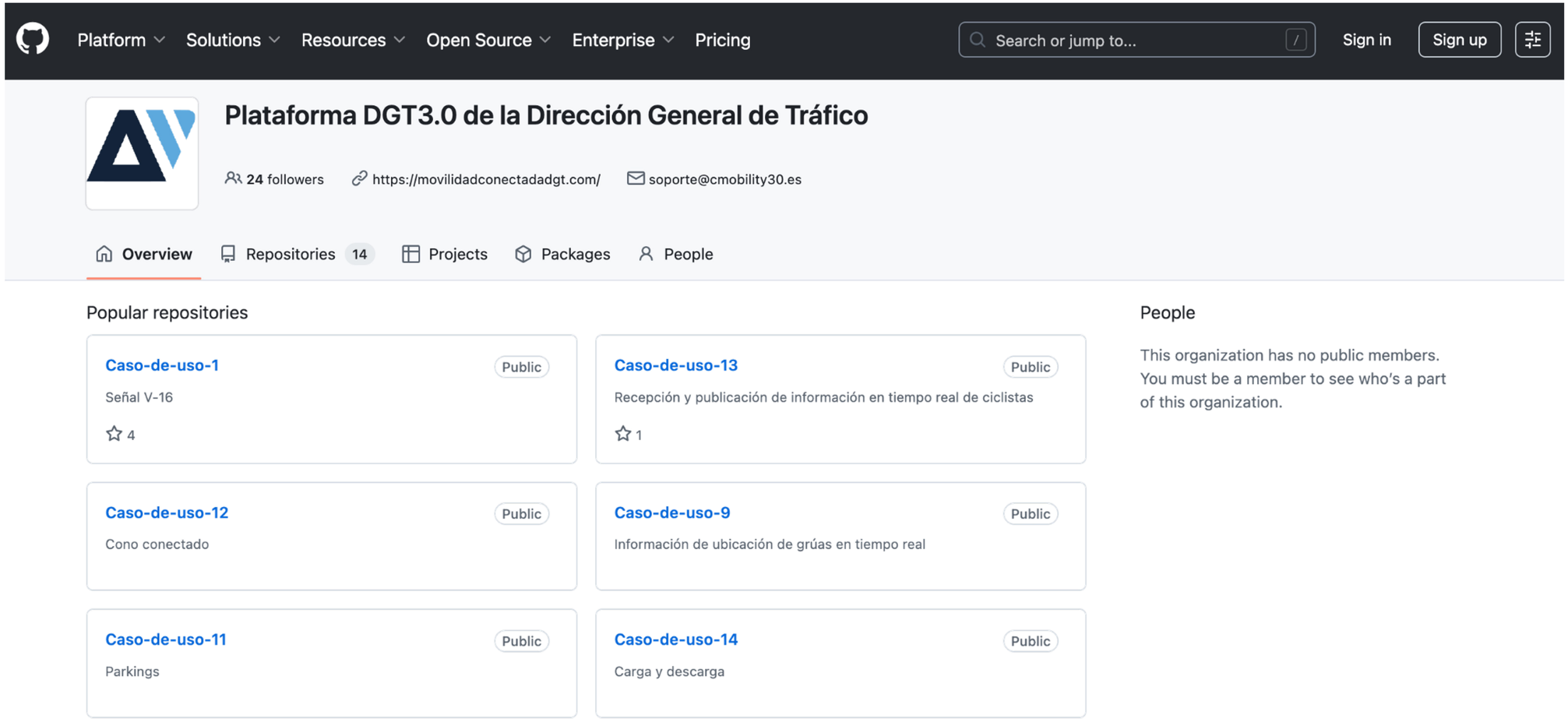
Acceso a la documentación técnica



Ba sde
htt
inr ado
ne

Acceso a la documentación técnica

Estos, nos llevan a https://github.com/dgt30-esp con los diferentes casos de uso asignados para cada una de ellas.



Acceso a la documentación técnica

Por ejemplo, tenemos el caso de los "**conos conectados**" similares a la V16 en https://github.com/dgt30-esp/Caso-de-uso-12/wiki donde se expone la publicación (endpoint del entorno con sus características) con sus tablas maestras y eventos (***todas ellas similares en todos los casos de uso***).

Esto nos lleva seriamente a pensar en que ***se han pensado casos de uso*** para **forzar luego a su explotación comercial** amparados por una Dirección General dependiente de un Ministerio Público.

Acceso a la documentación técnica

Por otra parte, para la suscripción es común en todos ellos realizar la conexión con la plataforma DGT 3.0 **a través de MQTT** (https://github.com/dgt30-esp/General/wiki/MQTT).

Es necesario o se rechazará la conexión:

- Dar de alta la **IP desde la que se solicita la conexión** (Consumidor/Publicador)
- Obtener las **credenciales MQTT** (Usuario y contraseña)
- Obtener un **ID de cliente**

Acceso a la documentación técnica

/Rooted

Para cumplir con estos requisitos será necesario **ponerse en contacto con la plataforma DGT 3.0** a través del email soporte@cmobility30.es del que era **propietario**…

DATOS DEL TITULAR	
Nombre del Dominio	cmobility30.es
Estado	Activado
Identificador	1A9BAD7-ESNIC-F5
Titular	Guilherme Ramos
Fecha de Alta	30-01-2019
Fecha de Caducidad	30-01-2026
Agente Registrador	GANDI

Acceso a la documentación técnica

/Rooted

Consulta realizada 15/02/2026

DATOS DEL TITULAR

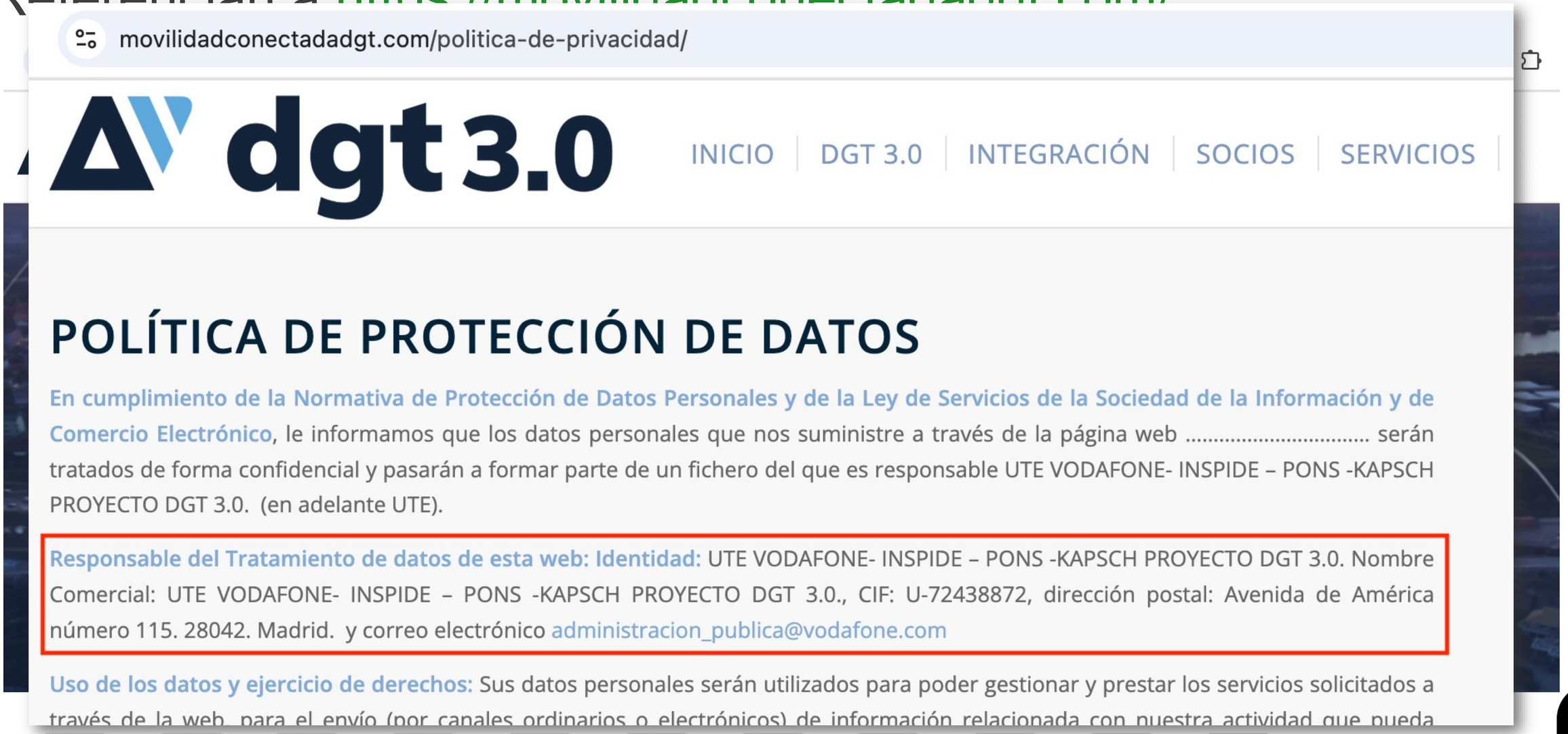
Nombre del Dominio	cmobility30.es
Estado	Activado
Identificador	1ACEE76-ESNIC-F5
Titular	JEFATURA CENTRAL DE TRÁFICO-MINISTERIO DEL INTERIOR
Fecha de Alta	30-01-2019
Fecha de Caducidad	30-01-2027
Agente Registrador	GANDI

3 3 7 12 1 9 1 14 1 11 1 6 1 18 1 14 1 4 1 7 1 3 0

Acceso a la documentación técnica

/Rooted

Referencian a https://movilidadconectadadgt.com/



3 3 8 12 1 9 1 14 1 11 1 6 1 18 1 14 1 4 1 7 1 3 0

Acceso a la documentación técnica

/Rooted

La señal V16 es el **caso de uso nº 1**

dgt30-esp / **Caso-de-uso-1** Public

Code | Pull requests | Actions | **Wiki** | Security | Insights

home

DGT 3.0 edited this page on Jun 24 · 18 revisions

Este caso de uso responde a la necesidad de cumplimentar lo regulado en la Instrucción 18/ V- 132 de la DGT y en el RD 159/2021, de 16 de marzo, por el que se regulan los servicios de auxilio en las vías públicas, en el que se obliga a los nuevos dispositivos de la señal V-16, a enviar un mensaje a la plaraforma DGT3.0. Se detalla por tanto, la comunicación entre la nube del fabricante de estos dispositivos y la plataforma DGT3.0

Todas las peticiones que se realicen a la API deben ser enviadas a la siguiente URL (URL base):

> https://pre.cmobility30.es/v16/

Publicación

Para **publicar** información se dispone una API REST:

3 3 9 12 1 9 1 14 1 11 1 6 1 18 1 14 1 4 1 7 1 3 0

Acceso a la documentación técnica

/Rooted

El acceso es por **HTTPS** y no por HTTP empleando un Certificado de **Let's Encrypt** (**no válido por eIDAS 2.0** - Reglamento (UE) 2024/1183 vigente desde el 20/05/2024 como ampliación al Reglamento 910/2014)

Resuelve a las direcciones IPv4 **34.249.188.44**, **52.51.4.181** y **54.72.61.0** localizadas en **eu-west-1** de **Amazon AWS**.

Hay otros subdominios asociados a **cmobility30.es** supuestamente en "**pro**" como **production.cmobility30.es** (52.48.39.203, 34.241.217.15 y 52.214.39.105 de AWS, eu-west-1)

El historial de certificados revela desarrollos https://crt.sh/?q=cmobility30.es





Acceso a la documentación técnica

/Rooted

crt.sh Identity Search

Group by Issuer

Criteria	Type: Identity Match: ILIKE Search: 'cmobility30.es'

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
23568325221	2026-01-05	2026-01-05	2026-04-05	cmobility30.es	cmobility30.es	C=US, O=Let's Encrypt, CN=R12
23568322054	2026-01-05	2026-01-05	2026-04-05	cmobility30.es	cmobility30.es	C=US, O=Let's Encrypt, CN=R12
23568342387	2026-01-05	2026-01-05	2026-04-05	v16.dev.cmobility30.es	v16.dev.cmobility30.es	C=US, O=Let's Encrypt, CN=R13
23568343635	2026-01-05	2026-01-05	2026-04-05	pre.cmobility30.es	pre.cmobility30.es	C=US, O=Let's Encrypt, CN=R13
23568324570	2026-01-05	2026-01-05	2026-04-05	v16.pre.cmobility30.es	v16.pre.cmobility30.es	C=US, O=Let's Encrypt, CN=R12
23568344381	2026-01-05	2026-01-05	2026-04-05	pre.cmobility30.es	pre.cmobility30.es	C=US, O=Let's Encrypt, CN=R13
23568322486	2026-01-05	2026-01-05	2026-04-05	v16.pre.cmobility30.es	v16.pre.cmobility30.es	C=US, O=Let's Encrypt, CN=R12
23568316707	2026-01-05	2026-01-05	2026-04-05	v16.dev.cmobility30.es	v16.dev.cmobility30.es	C=US, O=Let's Encrypt, CN=R13
23568340299	2026-01-05	2026-01-05	2026-04-05	dev.cmobility30.es	dev.cmobility30.es	C=US, O=Let's Encrypt, CN=R13
23568344696	2026-01-05	2026-01-05	2026-04-05	dev.cmobility30.es	dev.cmobility30.es	C=US, O=Let's Encrypt, CN=R13
23568322833	2026-01-05	2026-01-05	2026-04-05	v16.cmobility30.es	v16.cmobility30.es	C=US, O=Let's Encrypt, CN=R12
23568322134	2026-01-05	2026-01-05	2026-04-05	v16.cmobility30.es	v16.cmobility30.es	C=US, O=Let's Encrypt, CN=R12
22181128118	2025-11-03	2025-11-03	2026-02-01	v16.cmobility30.es	v16.cmobility30.es	C=US, O=Let's Encrypt, CN=R13
22181131792	2025-11-03	2025-11-03	2026-02-01	v16.cmobility30.es	v16.cmobility30.es	C=US, O=Let's Encrypt, CN=R13
22181126871	2025-11-03	2025-11-03	2026-02-01	dev.cmobility30.es	dev.cmobility30.es	C=US, O=Let's Encrypt, CN=R13
22181126872	2025-11-03	2025-11-03	2026-02-01	v16.dev.cmobility30.es	v16.dev.cmobility30.es	C=US, O=Let's Encrypt, CN=R13
22181131366	2025-11-03	2025-11-03	2026-02-01	v16.dev.cmobility30.es	v16.dev.cmobility30.es	C=US, O=Let's Encrypt, CN=R13
22181126959	2025-11-03	2025-11-03	2026-02-01	pre.cmobility30.es	pre.cmobility30.es	C=US, O=Let's Encrypt, CN=R12
22181131637	2025-11-03	2025-11-03	2026-02-01	dev.cmobility30.es	dev.cmobility30.es	C=US, O=Let's Encrypt, CN=R13
22181130131	2025-11-03	2025-11-03	2026-02-01	pre.cmobility30.es	pre.cmobility30.es	C=US, O=Let's Encrypt, CN=R12
22181127233	2025-11-03	2025-11-03	2026-02-01	v16.pre.cmobility30.es	v16.pre.cmobility30.es	C=US, O=Let's Encrypt, CN=R12
22181130677	2025-11-03	2025-11-03	2026-02-01	v16.pre.cmobility30.es	v16.pre.cmobility30.es	C=US, O=Let's Encrypt, CN=R12
22181126643	2025-11-03	2025-11-03	2026-02-01	cmobility30.es	cmobility30.es	C=US, O=Let's Encrypt, CN=R13
22181130263	2025-11-03	2025-11-03	2026-02-01	cmobility30.es	cmobility30.es	C=US, O=Let's Encrypt, CN=R13
21758399135	2025-10-16	2025-10-16	2026-01-14	dev.cmobility30.es	dev.cmobility30.es	C=US, O=Let's Encrypt, CN=R12
21758397357	2025-10-16	2025-10-16	2026-01-14	dev.cmobility30.es	dev.cmobility30.es	C=US, O=Let's Encrypt, CN=R12

3 3 11 12 1 9 1 14 1 11 1 6 1 18 1 14 1 4 1 7 1 3 0

Acceso a la documentación técnica

53 subdominios únicos de **cmobility30.es** (08/12/2025)
57 subdominios únicos el 15/02/2026 con:

*.devops, a.cs, b.cs, bandejadesalida-dev, bandejadesalida-preprod, **borrar**, **borrarpre**, **cheddar**, cs, dev, dev16, development, **developmentttt**, devops, **dgt30infosemaforos-dev**, **dgt30infosemaforos-oat**, dgt30pocsrti-dev, dgt30v16input-dev, gitlab, gitlab.cs, grafana-dev, grafana-oat, interno-oat.pmvv, interno-preprod.pmvv, **interno-prod.pmvv**, interno, interno.pmvv-oat, interno.pmvv, kibana-dev, minio.cs, oat, pmvv-dev, pmvv-oat, pmvv-preprod, pmvv-prod, pmvv, pmvv.dev, pmvvdev, pre, preprod, prev16, prometheus-dev, prometheus-oat, registry.cs, rundeck.cs, stilton, testing-repo-dev, use-case-5-dev, use-case-5-oat, v16, v16.dev, v16.pre, vault.cs


GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
DGT
Dirección General de Tráfico
/Rooted
Plataforma DGT 3.0
Legislación aplicable
V16
CONECTADA
A DGT 3.0
Obligatoria desde
01/01/26
Dispositivo que aumenta tu seguridad.
Para vehículos inmovilizados en carretera.

Legislación aplicable

/Rooted

Todo estaba planeado, pero **un poco oculto** a la ciudadanía…

Instrucción 18/V-132

DGT Dirección General de Tráfico

21/12/2018

2019

2020

17/03/2021

BOLETÍN OFICIAL DEL ESTADO

R.D. 159/2021
Regulación de los servicios de auxilio en las vías públicas

Resolución 30/11 de la DGT
Protocolo y formato para el envío de datos

BOLETÍN OFICIAL DEL ESTADO

10/12/2021

20/12/2022

BOLETÍN OFICIAL DEL ESTADO

R.D. 1030/2022
Análisis de la efectividad de las comunicaciones y la conectividad de las señales V16

2023

2024

2025

Uso obligatorio



01/01/2026

3 3 12 12 1 9 1 14 1 11 1 6 1 18 1 14 1 4 1 7 1 3 0

Legislación aplicable

Instrucción 18/ V- 132 de la DGT de 2018
https://www.dgt.es/export/sites/web-DGT/.galleries/downloads/muevete-con-seguridad/normas-de-trafico/VEH-vehiculos/Instruccion-18-V-132-Revision-senal-V16-2.pdf sobre "*Dispositivo luminoso vehículos inmovilizados en la vía., señal V16. Revisión características técnicas*".

Indicaba su **coexistencia con los triángulos de señalización**…

Legislación aplicable

"***Opcionalmente***, ***además***, *podrá colocarse en el exterior del vehículo inmovilizado* ***un dispositivo luminoso de color amarillo*** *auto que tenga las siguientes características...*"

En la misma, se exponía "*se están llevando a cabo los preparativos para modificar el Anexo XI, apartado 4 de la señal V16, del Real Decreto 2822/1998*"

Por lo que todo **apuntaba a que sería regulada**…

Legislación aplicable

R.D. 159/2021, de 16 de marzo, por el que **se regulan los servicios de auxilio en las vías públicas** disponible en https://www.boe.es/boe/dias/2021/03/17/pdfs/BOE-A-2021-4194.pdf en su Disposición final segunda "*Modificación del Reglamento General de Vehículos aprobado por Real Decreto 2822/1998, de 23 de diciembre*", en su punto Cinco redacta las **especificaciones técnicas** de esta señal.

Legislación aplicable

Con independencia de otras características, nos interesa:

*4. Este dispositivo comunicará, en todo caso, su **activación, desactivación y geoposicionamiento**, al punto de acceso nacional en materia de tráfico y movilidad. La información sobre la ubicación del vehículo accidentado **se enviará cada 100 segundos** y dejará de enviarse una vez se haya remitido la información de desactivación.*

*5. El coste las comunicaciones estará incluido en el precio de venta al público y estas se garantizarán durante **al menos 12 años**.*

*6. El dispositivo **incluirá en el interior de su carcasa todos los elementos necesarios para su operación**, incluidos los de comunicaciones, sin depender en ningún caso de elementos externos como aplicaciones de teléfonos móviles u otros similares.*

Legislación aplicable

En su Disposición final tercera "***Protocolo y formato de conexión con el punto de acceso nacional de tráfico y movilidad***" se indica textualmente que:

> "*En el plazo máximo de un año desde la entrada en vigor del presente real decreto, el titular de la Dirección General de Tráfico aprobará, por medio de una resolución, el protocolo y el formato de envío de los datos requeridos por parte de los servicios de auxilio en carretera y de la señal V16 a los efectos de su publicación en el punto de acceso nacional en materia de tráfico y movilidad*".

Legislación aplicable

Resolución de 30 de noviembre de 2021, de la Dirección General de Tráfico, por la que ***se define el protocolo y el formato para el envío de datos desde la señal V16 al Punto de Acceso Nacional***, en el ámbito de la Directiva 2010/40/UE del Parlamento Europeo y del Consejo, de 7 de julio de 2010, por la que se establece el marco para la implantación de los sistemas de transporte inteligente en el sector del transporte por carretera (BOE nº 295, de 10 de diciembre de 2021)
https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-20433

Legislación aplicable

R.D. 1030/2022, de 20 de diciembre (https://www.boe.es/buscar/doc.php?id=BOE-A-2022-21683), por el que se modifica el Real Decreto 159/2021 anterior, de 16 de marzo, por el que se regulan los servicios de auxilio en las vías públicas donde se añaden apartados a los dispositivos de señalización de peligro y que entre otros, ***exigen incluir el análisis de la efectividad de las comunicaciones, así como la conectividad de las señales V16***, con la plataforma de vehículo conectado de la Dirección General de Tráfico.

Legislación aplicable

Tal como se indica, desde la propia página https://www.dgt.es/muevete-con-seguridad/tecnologia-e-innov se puede **tivos V16**

Por ***los dispo*** y los "**Escr**

MOTOR

La Unión Europea podría tumbar la norma de la baliza V-16

Según el PPE (Partido Popular Europeo), la Comisión Europea dice que España no comunicó la norma de la baliza V-16 y advierte sobre las consecuencias jurídicas. Ningun otro país de Europa la usa.


GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
DGT
Dirección General de Tráfico
/Rooted
Plataforma DGT 3.0
Protocolos y mensajes de la señal V16
V16
CONECTADA
A DGT 3.0
Obligatoria desde
01/01/26
Dispositivo que aumenta tu seguridad.
Para vehículos inmovilizados en carretera.

Protocolos y mensajes de la señal V16

Resolución de 30 de noviembre de 2021 de la Dirección General de Tráfico, por la que se define el protocolo y el formato para el envío de datos desde la señal V16 al Punto de Acceso Nacional.

- **Anexo I**: Protocolo de ***especificaciones técnicas*** para la conectividad de la señal V16 con el Punto de Acceso Nacional.

- **Anexo II**: Requisitos en materia de ***comunicaciones***.

Protocolos y mensajes de la señal V16

Del primero, se tienen los **requisitos para los fabricantes**:

a) Acceder a la plataforma de gestión del Punto de Acceso Nacional (NAP) mediante certificado digital proporcionado por la Dirección General de Tráfico.
b) Implementar los protocolos e interfaces descritos en esta resolución para el envío de los mensajes generados por la señal V16.
c) Enviar un mensaje de activación y otro de desactivación del dispositivo por cada evento.
d) Enviar la señal de activación 100 segundos después del encendido físico del dispositivo.

Protocolos y mensajes de la señal V16

e) Mantener una frecuencia de envío de mensajes cada 100 segundos.
f) Proporcionar una precisión inferior a 5 metros en el posicionamiento del dispositivo.

En este punto, surge la duda razonable del apartado c) en cuanto al **mensaje de desactivación** del dispositivo por cada evento, ya que imaginemos que ***no se produce nunca*** porque nos quedamos sin batería, fuera de cobertura, etc...

Protocolos y mensajes de la señal V16

/Rooted

También se definen **2 protocolos** (**A** y **B**) para los dispositivos:

- '**A**' es para el envío de datos **de la señal a los fabricantes**.
- '**B**' entre **los fabricantes y el punto nacional** (NAP)

Se cita que toda la documentación técnica actualizada se encontrará recogida en la página web www.dgt.es/v16

Protocolos y mensajes de la señal V16

En cuanto al **protocolo 'A' (baliza -> fabricante)**, se define el **modelo de datos común**. ***Esto no quita que algún fabricante pueda implementar más datos*.**

Se indica que, en caso de la existencia de alguna problemática sobrevenida a los sistemas de información de algún fabricante, ***un tercero pueda realizar dichas funciones***, es decir, si el fabricante 'desaparece' del mercado, se puede asegurar que la señal lo enviará a otro que asumirá dichas funciones.

Protocolos y mensajes de la señal V16

/Rooted

El modelo de datos que se define es:

Campo	Descripción
Longitud.	Longitud de la trama actual.
Versión.	Versión de la trama.
Tipo de Trama.	Tipo de Trama que será: 0= Inicio de incidencia. 1=Incidencia. 2 =Fin de incidencia.
Secuencia.	Número secuencial de la trama. Este número se incrementará con cada trama transmitida. La secuencia se reiniciará por un nuevo incidente.
ID del fabricante.	Identificador del fabricante.
Versión SW.	Versión de software.
Versión HW.	Versión de hardware.
ID del dispositivo.	Número entero que identificará inequívocamente al dispositivo.
Batería.	Número de Voltios multiplicado por diez, en formato entero.
Tiempo Activación.	Tiempo que el dispositivo lleva activado en minutos.
IMEI.	Cadena de caracteres ASCII. IMEI="xxxxxxxxxxxxxxx".
Número de celda «+» número de ECL.	ID de la celda 30 bit «+» ECL.

Protocolos y mensajes de la señal V16

/Rooted

Campo	Descripción
RSSI.	Received signal strength level.
RSRP.	Reference signal received power.
RSRQ.	Reference signal received quality.
PLMN.	PLMN (Public Land Mobile Network). Cadena ASCII 5 a 6 dígitos (MCC MNC).
Auxiliar.	Campo auxiliar reservado para posibles usos futuros.
NS.	N (Norte) o S (Sur) (1 caracter).
DD.DDDDDD.	Latitud Grados (DD.DDDDDD).
EW.	E (Este) o W (oeste) (1 caracter).
DDD.DDDDDD.	Longitud Grados (DDD.DDDDDD).
Timestamp.	YYYYMMDDHHMISS UTC GPS TIMESTAMP.
Altitud.	Metros, entero.
EPE_horiz.	Error de posición horizontal (metros), entero.
Satélites.	Numero de satélites.
HDOP.	Horizontal dilution of precision multiplicado por cien, en formato entero.



Protocolos y mensajes de la señal V16

Todos los atributos se enviarán en **formato texto**.

El protocolo incluirá un **paquete UDP de respuesta** (acuse de recibo) por parte del operador de telefonía, que el fabricante podrá utilizar a efectos de control de llegada del paquete, ya que el protocolo UDP no dispone de esta característica.

> *La determinación final ha sido **no incluirlo** y darlo por recibido si se ha publicado (tipo acuse de recibo en vez de dicho paquete).*

Protocolos y mensajes de la señal V16

/Rooted

En cuanto al **protocolo 'B'** que es el empleado entre el

Campo	Descripción
idcompany.	Nombre del certificado de cliente (Common Name, CN).
actionid.	Identificador único del evento anonimizando al dispositivo de origen, desde la activación a la desactivación.
token.	Identificador cifrado generada por la plataforma de vehículo conectado DGT 3.0 para la plataforma cliente durante el proceso de autenticación.
detection_time.	Timestamp del instante en el que ocurre el evento, en formato ISO 8601 YYYY-MM-DDTHH:MM:SSZ.
lon.	Longitud geográfica del evento en coordenadas WGS84.
lat.	Latitud geográfica del evento en coordenada WGS84.
device_event_type.	Tipo de evento: 1 – Vehículo detenido.
device_event_type_value.	Valor del tipo de evento: 1 = activación. 2 = activado. 3 = desactivación.
information_quality.	Precisión GPS estimada en metros (HDOP).

Protocolos y mensajes de la señal V16

Para el **posicionamiento**, de acuerdo con el Real Decreto 1071/2007 de 27 de julio, deben expresarse las coordenadas en grados sexagesimales, con 5 decimales, en el ***sistema de referencia ETRS89***.

Se empleará la **escala de tiempo UTC** independiente de zonas horarias.

La **sincronización** entre los dispositivos implicados en el tratamiento, se realizará usando el protocolo **NTP (Network Time Protocol)** con **hora.roa.es**

Protocolos y mensajes de la señal V16

En el **Anexo II**, se definen los **requisitos de comunicaciones**, donde se requiere el uso de **tecnología celular en banda licenciada** para evitar interferencias del servicio, contemplada dentro de los estándares ***4G/5G LPWA de la GSMA***, garantizando la permanencia en funcionamiento de dicha tecnología durante el transcurso del tiempo y la no obsolescencia temprana.

Protocolos y mensajes de la señal V16

/Rooted

La gestión, seguridad y privacidad en las comunicaciones obliga a emplear:

- Entorno **privado y seguro de comunicaciones** (APN privado).
- Utilización de tarjeta **SIM no extraíble** para evitar manipulaciones.
- **Provisión automática** y **desatendida** para evitar procedimientos de activación intermedios que puedan interferir en el momento de un accidente o avería.

Protocolos y mensajes de la señal V16

/Rooted

- El fabricante del dispositivo V16 dispondrá de una herramienta de **gestión de alarmas** para el **control del fraude** por malos usos con posibilidad de ***bloqueo automático de las comunicaciones***, que será **provista por el operador de comunicaciones** que preste el servicio de conectividad.
- Contrato de servicio de comunicaciones con el operador incluidas, en **modo prepago**, ***por doce años***.

Protocolos y mensajes de la señal V16

La **validación de los dispositivos**, queda fuera del estudio, aunque destaca que "se deben utilizar ***protocolo de comunicaciones estándar UDP*** con el fin de garantizar la intercambiabilidad del servicio prestado”.

Finalmente, se hace mención a las **evoluciones tecnológicas** donde destaca la ***retrocompatibilidad con los protocolos del Anexo I***, la cobertura que será ***equivalente a la ofrecida por las tecnologías celulares en cada momento*** y que, se deberá **garantizar la disponibilidad** del canal para el intercambio de mensajes.


GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
DGT
Dirección General de Tráfico
/Rooted
Plataforma DGT 3.0
API Rest para el envío de eventos
V16
CONECTADA
A DGT 3.0
Obligatoria desde
01/01/26
Dispositivo que aumenta tu seguridad.
Para vehículos inmovilizados en carretera.

API Rest para el envío de eventos

/Rooted

Las peticiones se dirigen a https://pre.cmobility30.es/v16/ y para publicar se dispone de un **API Rest** en **`{baseUrl}/v1/...`** donde:

- La API utiliza **JSON Web Tokens** para la ***autentificación***.
- Las **peticiones** de la API deben ser realizadas con peticiones ***GET*** o ***POST*** según el caso.
- Se pueden considerar todas las **respuestas que no sean** devueltas con un código ***HTTP 200*** como un ***error***.
- Todas las respuestas son en **formato JSON**.

API Rest para el envío de eventos

Autenticación (basada en el **campo `'cn'`** del Certificado Cliente):

El endpoint es **`{baseUrl}/v1/token`** y devuelve un JSON como:

```
{
    "issuedAt": "2026-02-07T09:09:16.284Z",
    "expiration": "2026-02-07T09:09:16.284Z",
    "token": "Bearer eyJhbGciOiJIUzUxMiJ9.e....."
}
```

El algoritmo empleado en el JWT es **HS512** y las peticiones al API, viajan cifradas con una capa de seguridad TLS.

API Rest para el envío de eventos

Cualquier petición posterior, es mediante la cabecera `Authorization` con el `Bearer` del token, que caduca de forma aleatoria a lo largo de la misma (***actualmente es de 1 día***).

Si la petición es con un **token expirado** se recibe un error `HTTP 400 - Bad Request` y debe ***obtenerse un nuevo token***.

API Rest para el envío de eventos

Mediante las tablas maestras descritas, podemos obtener la **información relevante para los eventos**, ya que, en el API, el evento es la parte principal para la ingesta de datos.

Tipos de Eventos

Método: **GET**

URL: `{baseUrl}/v1/mastertables/device_event_types`

Valores de los tipos de eventos

Método: **GET**

URL: `{baseUrl}/v1/mastertables/device_event_types_values`

API Rest para el envío de eventos

Tipos de informaciones devueltas

Método: **GET**
URL: `{baseUrl}/v1/mastertables/infos`

Obtención del id de empresa

Método: **GET**
URL: `{baseUrl}/v1/idcompany`

Es aquí donde se enviará la información a la plataforma y su uso es al endpoint `{baseUrl}/v1/postincidence` mediante el método **POST**.

API Rest para el envío de eventos

/Rooted

En el cuerpo, se indicará un **JSON con los atributos** a enviar:

```
{
  "actionid": "1",
  "detection_time": "2026-02-07T12:13:37Z",
  "lon": -3.79465,
  "lat": 40.39485,
  "device_event_type": 1,
  "device_event_type_value": 1,
  "information_quality": 1
}
```




API Rest para el envío de eventos

Existen unos requisitos para los mensajes, como:

- La posición geográfica debe estar contenida en el **territorio español**.
- La posición proporcionada por el GPS **no debe tener un error mayor a 5 metros**.
- Se aceptarán eventos con una **antigüedad máxima de 15 segundos con respecto a la hora UTC**, y que no sea un dato a futuro.
- El atributo `actionid`, debe ser un **identificador único** para toda la vida de la incidencia que se reporta desde el dispositivo y para esa `idcompany`.

API Rest para el envío de eventos

El **protocolo de comunicación** es muy sencillo:

- Se envía evento de "**Activación**" ***100 segundos después del encendido físico*** del dispositivo.
- Se envía(n) evento(s) **cada 100 segundos** entre mensajes de evento "**Activado**".
- Se envía evento de "**Desactivación**".

API Rest para el envío de eventos

/Rooted

El mecanismo **idaction** con el **idcompany** se deja libre a los desarrolladores por lo que no existe una "**estandarización real**", pero el único común es el 1 (detención).

- ✓ **No existe información de datos personales que puedan identificar de algún modo al vehículo o conductor**.
- ✓ La señal o su protocolo **tampoco comunican ninguna información a servicios de emergencia** (112...), Fuerzas y Cuerpos de seguridad o a la asistencia en carretera. Será el usuario quien tenga que advertir por otro medio la comunicación necesaria al receptor adecuado.

API Rest para el envío de eventos

La plataforma del fabricante no tiene por qué implementar una **política de reenvíos de mensajes** en caso de que la plataforma DGT 3.0 deje de prestar servicio temporalmente ya que la misma, tiene una ***política de retención de los mensajes*** en función de su riesgo.

Al ser escalable y conocido el tiempo y número máximo de mensajes a recibir, la plataforma DGT 3.0 **no sería susceptible de ataques de denegación de servicio (DDoS)** pero se desconoce si se ha impuesto algún tipo de ***rate-limit*** o incluso bloqueo selectivo de ciertos `idcompany`.

API Rest para el envío de eventos

Desde el punto de vista del desarrollo, se agradecería un **formato unificado en lowerCamelCase** para los endpoints y atributos, donde la primera palabra comienza con minúscula y las palabras subsiguientes comienzan con mayúscula, sin usar espacios ni guiones bajos.


GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
DGT
Dirección General de Tráfico
/Rooted
Señal V16
Funcionamiento
V16
CONECTADA
A DGT 3.0
Obligatoria desde
01/01/26
Dispositivo que aumenta tu seguridad.
Para vehículos inmovilizados en carretera.

Señal V16: funcionamiento

La baliza V16 incluye en su interior **todos los elementos necesarios para su correcto funcionamiento**, incluido un chip **GPS**, un **modem 4G/5G** y una tarjeta **SIM no extraíble** con ***prepago de 12 años*** al operador, además de los **dispositivos lumínicos necesarios** y la **electrónica de control necesaria** alimentada por **pilas** o **baterías** (que se autoriza en contra de lo que se escucha principalmente en RR.SS.)

Una vez activada transmite su posición a los 100 segundos, **nunca antes**, por lo que se puede llevar perfectamente sin las pilas puestas. La obligación del usuario es que cuando se active, funcione.

3 3 12 12 9 9 14 14 11 11 1 6 1 18 1 14 1 4 1 7 1 3 0

Señal V16: funcionamiento

El **GPS recibe su posición de los satélites disponibles en su área de cobertura** (en este caso, al igual que ocurre con los tradicionales, hay zonas donde no se reciben bien y no son precisos como en túneles...) y dependerá de la calidad de los componentes empleados en el dispositivo.

Hay que tener en cuenta que suelen 'recordar' la última posición donde tuvieron cobertura y que se necesitan varios satélites para su geolocalización, donde hasta que no estén todas las señales estabilizadas, **no podrá ofrecer una posición con precisión**.

Además, es en esto donde más batería se gasta.

Señal V16: funcionamiento

La unidad de control, recibe dichos datos y los normaliza para enviarlos a través del modem integrado junto con otros necesarios a una red **NB-IoT/LTE-M (4G/5G LPWA de 3GPP) de telefonía** con un **APN privado** previsto para la tarjeta SIM integrada.

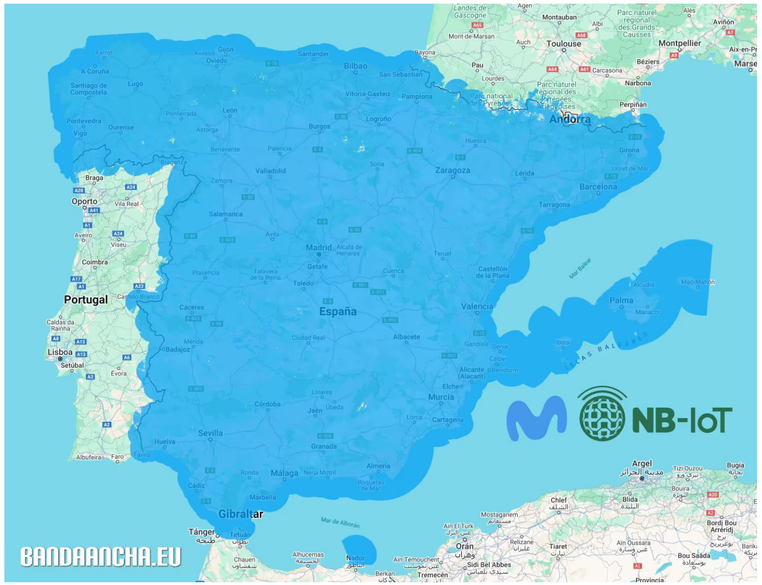
En ningún momento ***estos datos viajan por internet*** o incluso por una VPN de internet.

Estos a través de los repetidores y torretas **son recibidos por el fabricante de nuestra baliza** con el **protocolo 'A'**.

3 3 12 12 9 9 14 14 11 11 3 6 1 18 1 14 1 4 1 7 1 3 0

Señal V16: funcionamiento

Es necesario encontrarse en un **área de cobertura por parte del operador**.







Señal V16: funcionamiento

/Rooted

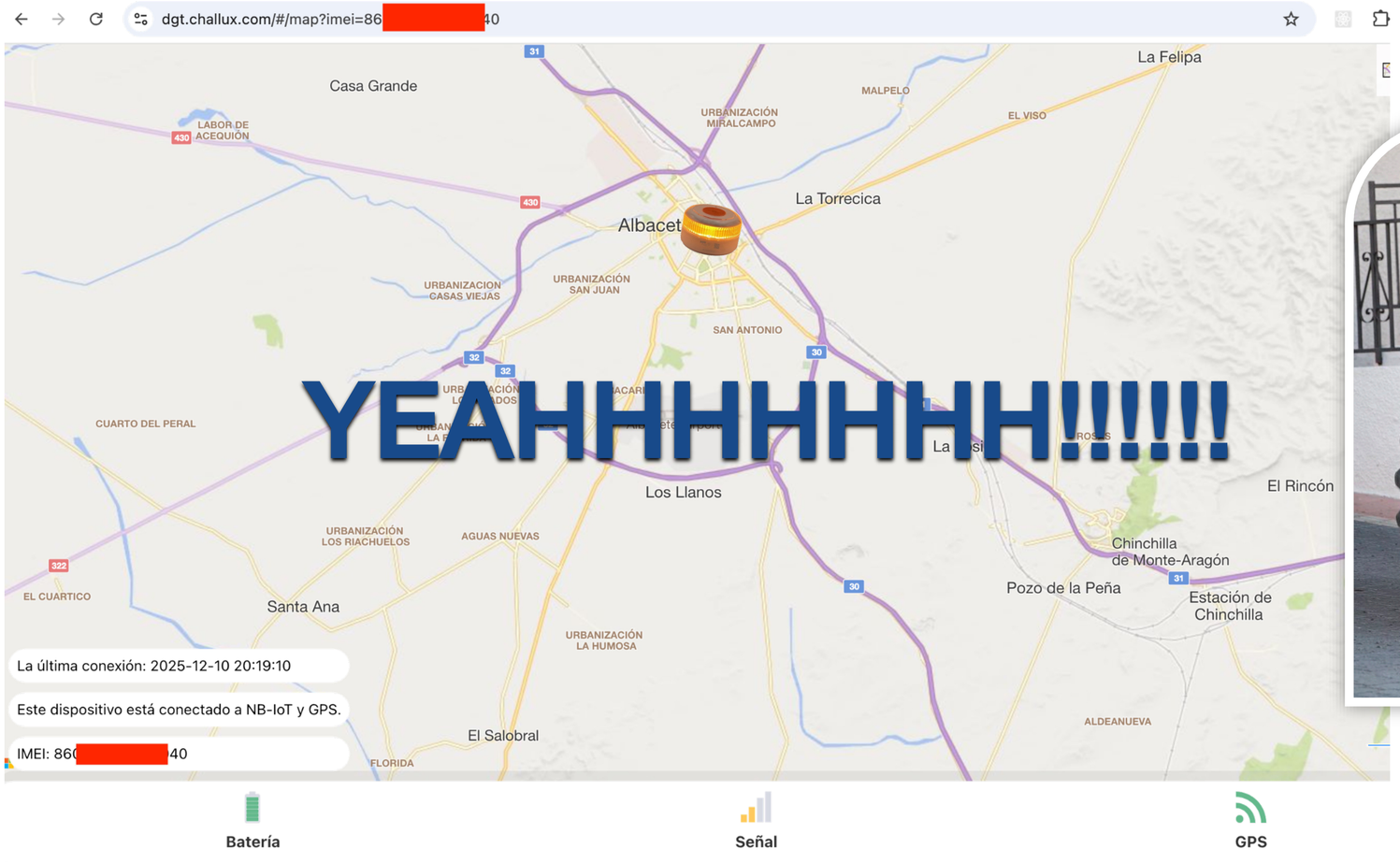
En ese momento, **el fabricante y vía internet** con una IP en whitelist y su Certificado Digital expedido por la CA de la DGT 3.0 inicia una ***comunicación con el APN*** empleando el **protocolo 'B'** y **reenvía los datos requeridos**.

Desde la **DGT 3.0 y una vez recibidos**, podrán a su vez ***reenviarse a navegadores, paneles, etc.*** para informar al resto de conductores.

la DGT dice textualmente que "**adicionalmente, se quiere trabajar el concepto de visibilidad virtual**", en definitiva, "**visibilidad física y visibilidad virtual**"

Señal V16: funcionamiento

¿Lo siguiente será **obligar al usuario** a incorporar ***visibilidad acústica con voces*** como el paisano?





3 3 12 12 9 9 14 14 11 11 6 6 1 18 1 14 1 4 1 7 1 3 0


GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
DGT
Dirección General de Tráfico
/Rooted
Señal V16
Componentes hardware
V16
CONECTADA
A DGT 3.0
Obligatoria desde
01/01/26
Dispositivo que aumenta tu seguridad.
Para vehículos inmovilizados en carretera.

Señal V16: componentes hardware

/Rooted

Existen **pocos fabricantes** pero **muchas marcas** y **modelos**.
https://www.dgt.es/muevete-con-seguridad/tecnologia-e-innovacion-en-carretera/Dispositivos-de-presenalizacion-V16/



Fecha de consulta: 15/02/2026





Señal V16: componentes hardware

/Rooted

34 fab

ATRES
DISTRI
DONGG
DONGG
ENERG
FOSHA
FOSHA
FUJIAN
HANGZ
HUIZHC
HUIZHC
HYBRID
KEPAR
MIROVI
NEOWA
NINGBC
NINGBC



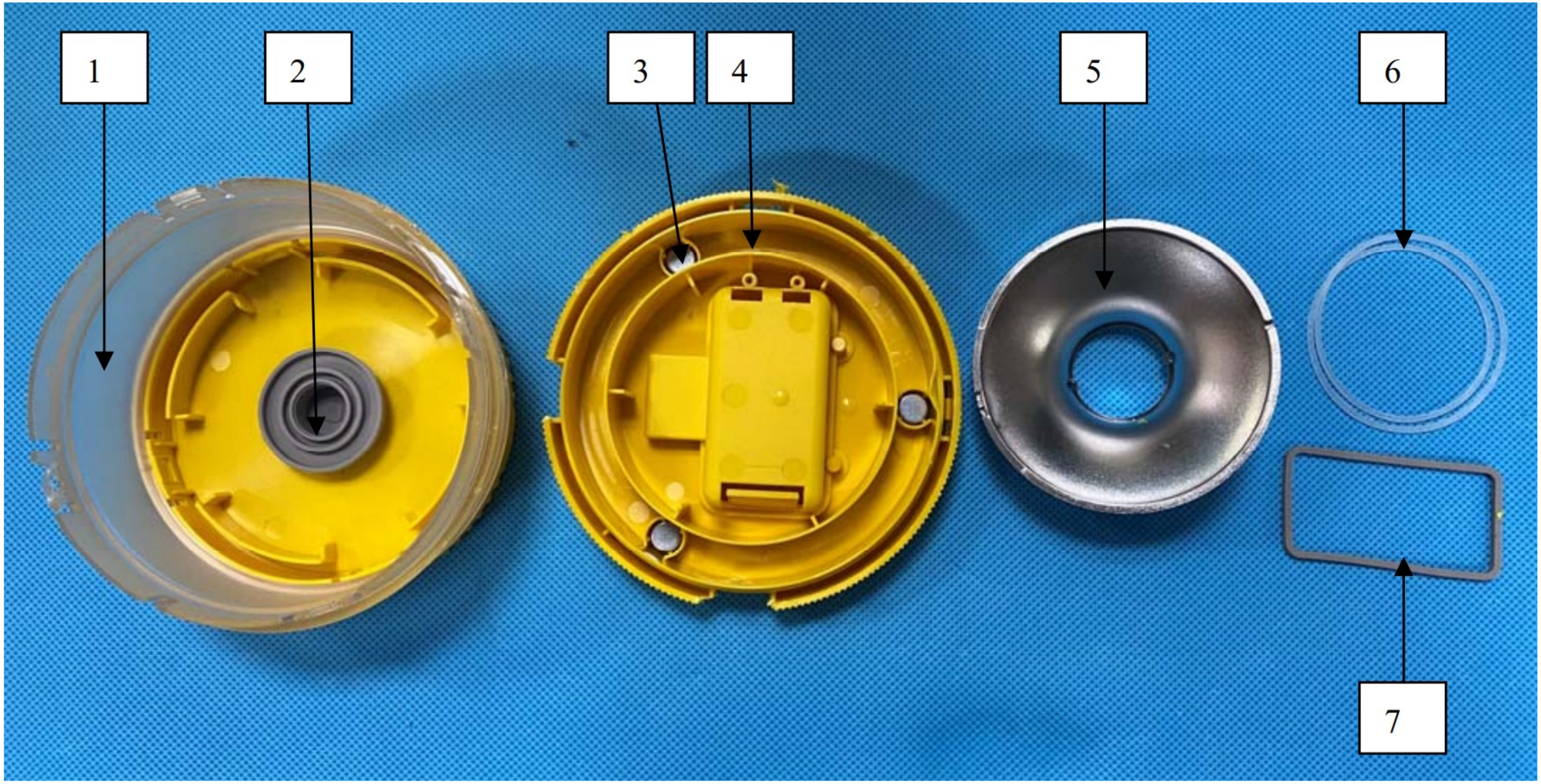
O., LTD
O., LTD
CO., LTD
CTORY
LTD
CO.,LTD
LOGY CO LTD

Señal V16: componentes hardware

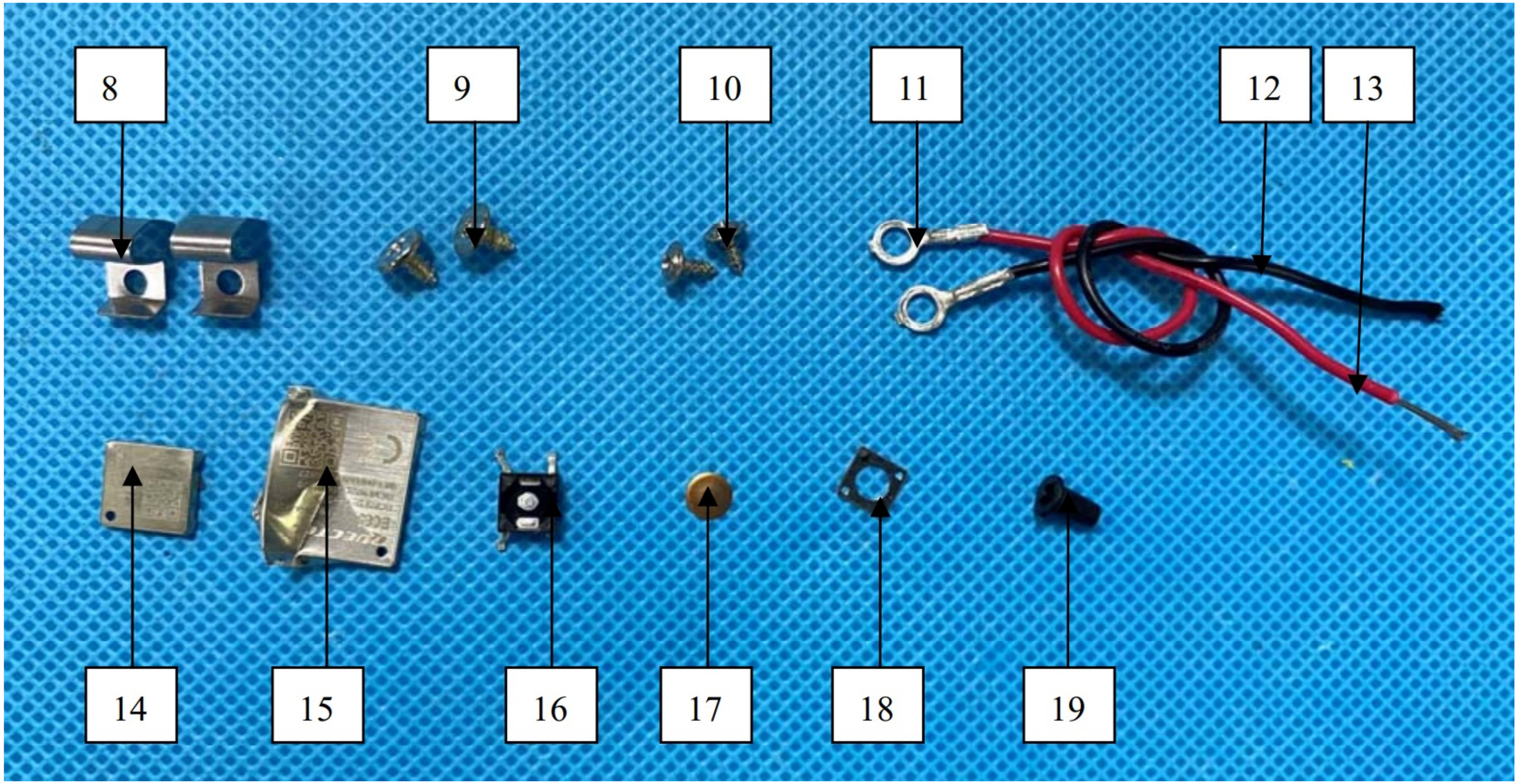
Componentes



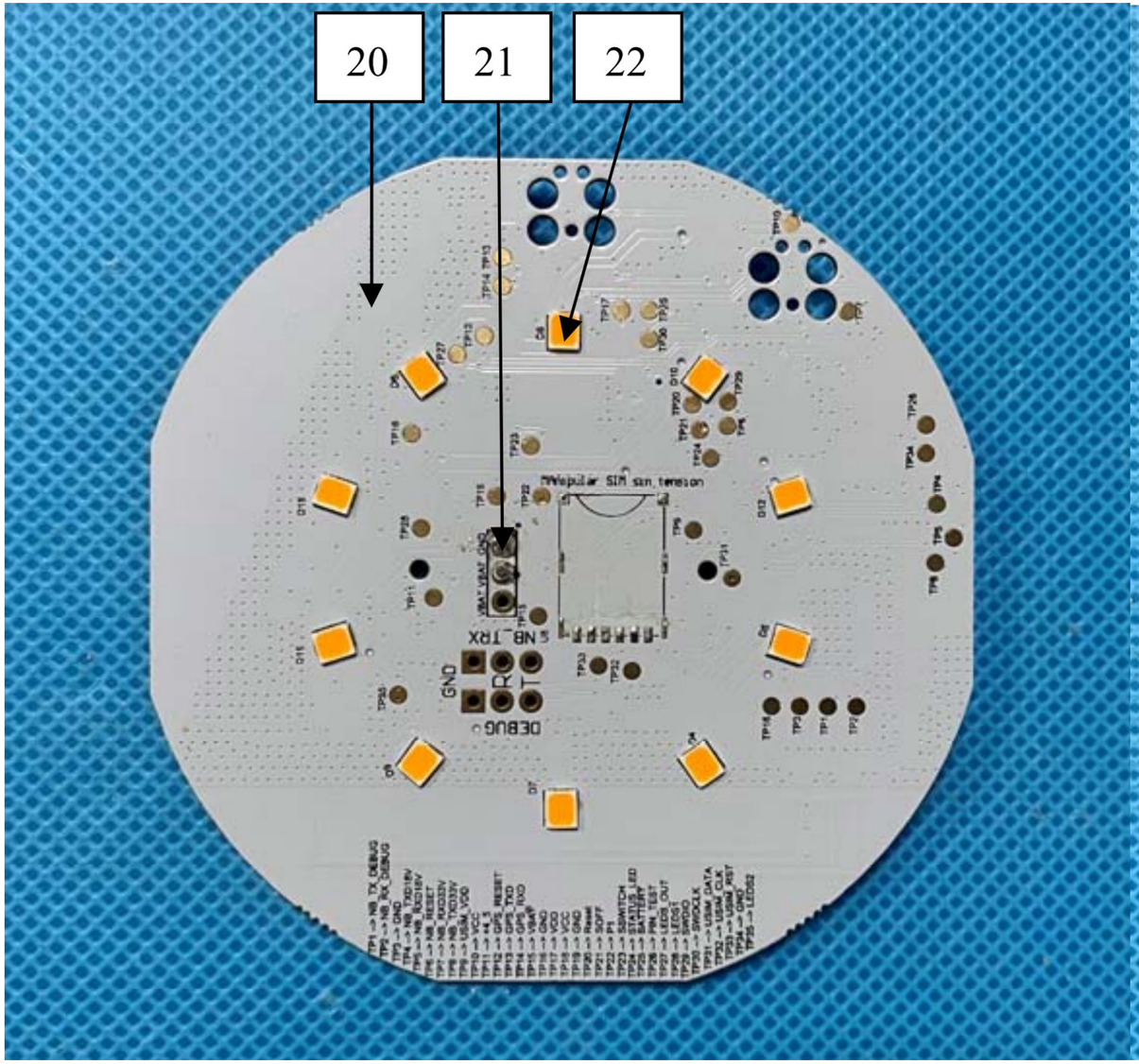
Señal V16: componentes hardware

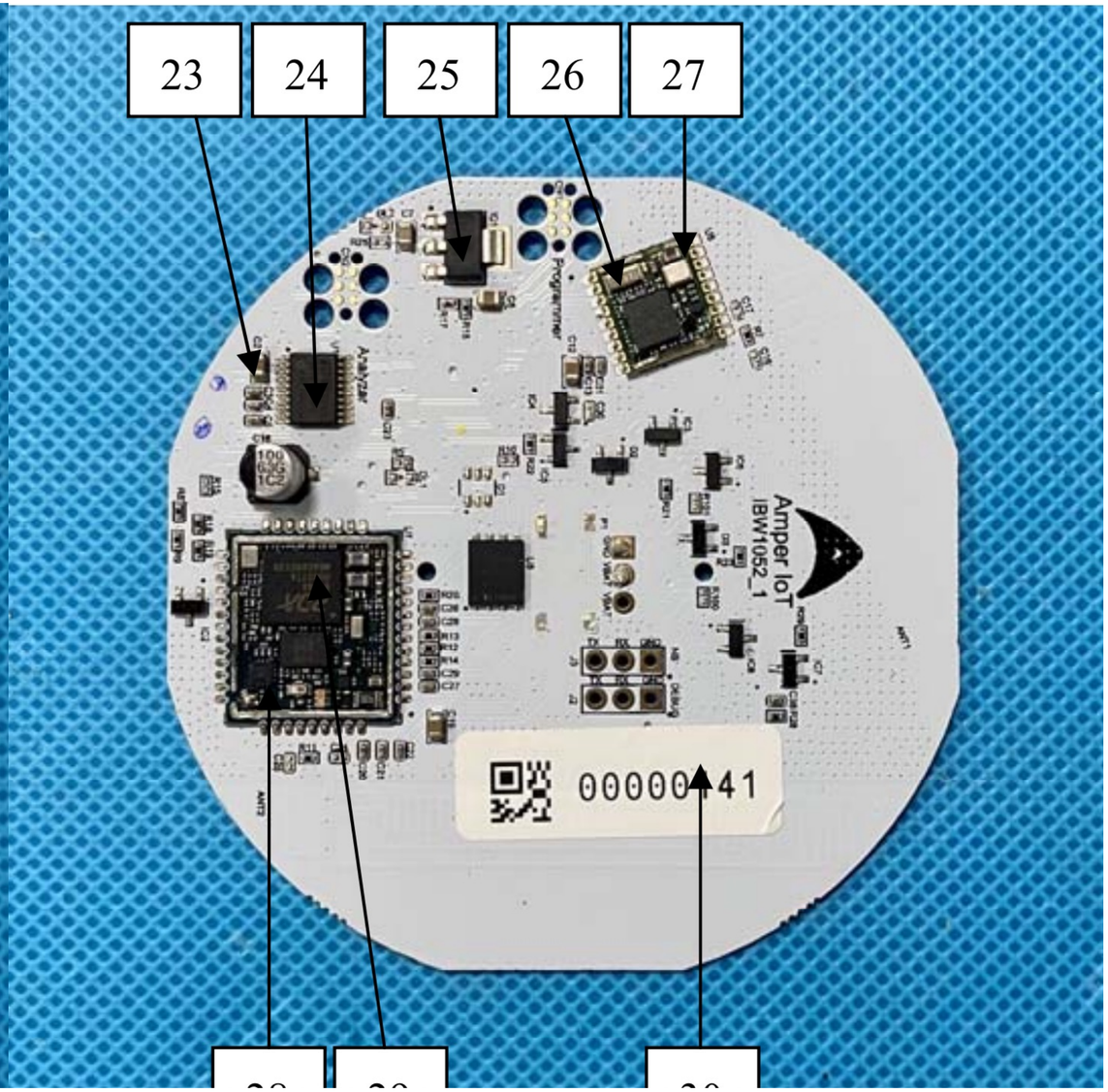


Señal V16: componentes hardware



Señal V16: componentes hardware

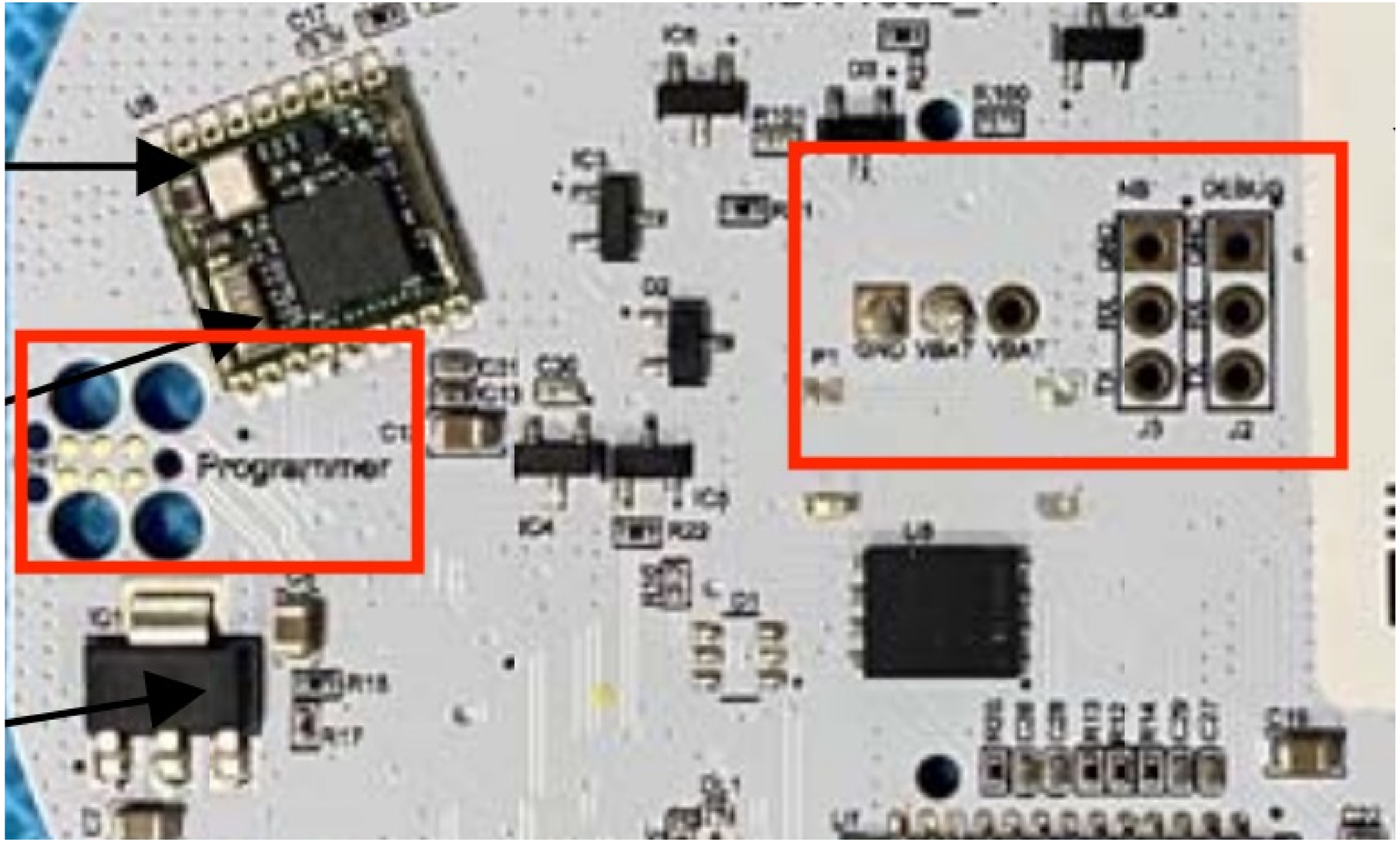




Señal V16: componentes hardware

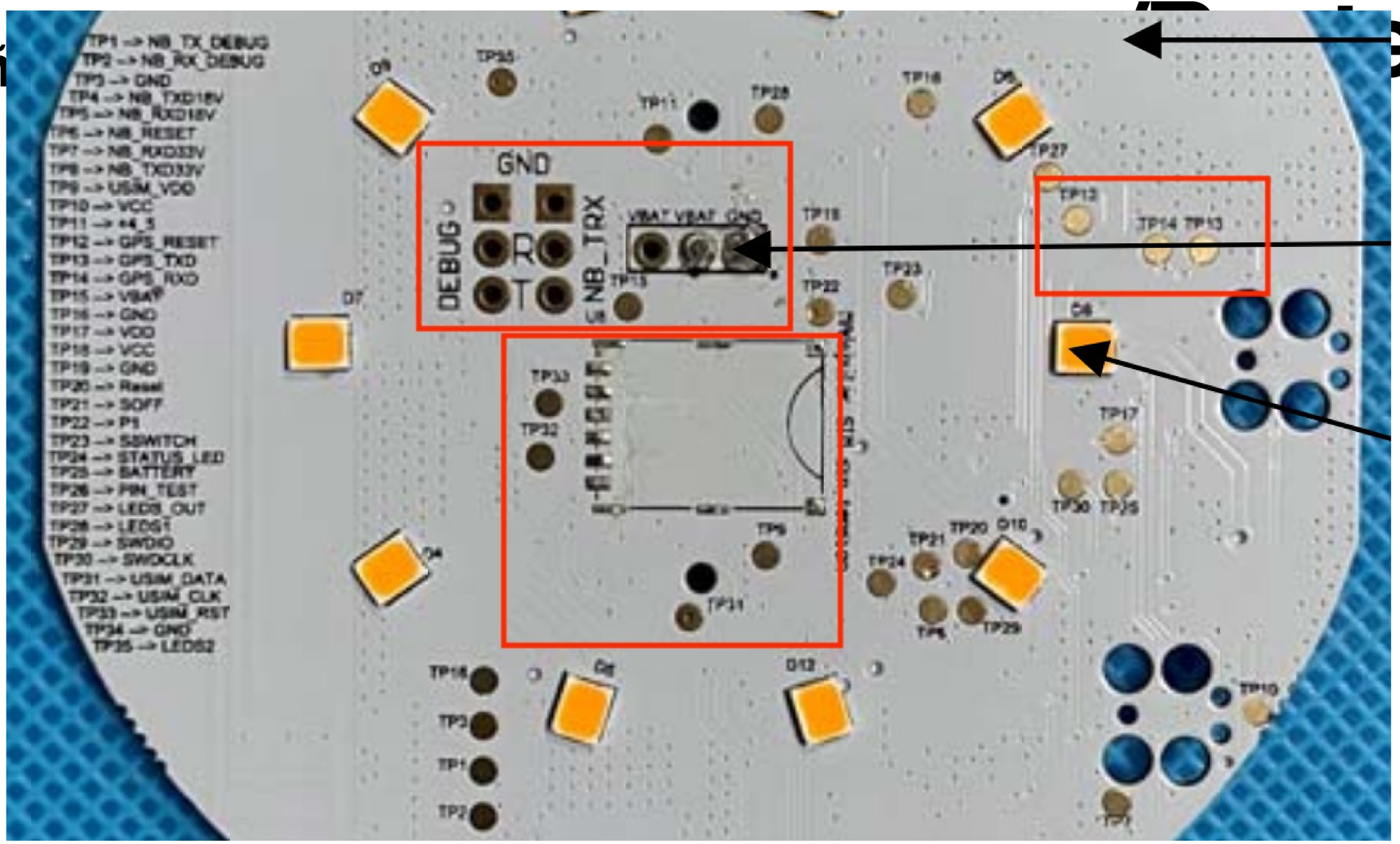
/Rooted

Test Points



Señ

Test Points



Señal V16: componentes hardware

JBM Ref. 54735 (Cert. IDIADA PC25020303)



SW Version: R1.10

Date: 25/11/2024

Photo:

ZHONGSHAN JUCAR ELECTRONIC TECHNOLOGY CO.,LTD - WL806GPS end device, in its R1.10 version, **is compatible** with Telefónica IoT/M2M solution according to specific functionalities tested in the mobile networks specified.

Some issues have been detected, they may affect device functionality and it is highly recommended to fix them.

ZHONGSHAN JUCAR ELECTRONIC TECHNOLOGY CO.,LTD shall deliver to Telefonica a solution plan to solve open issues.

Validate this repo
Verifique el inform

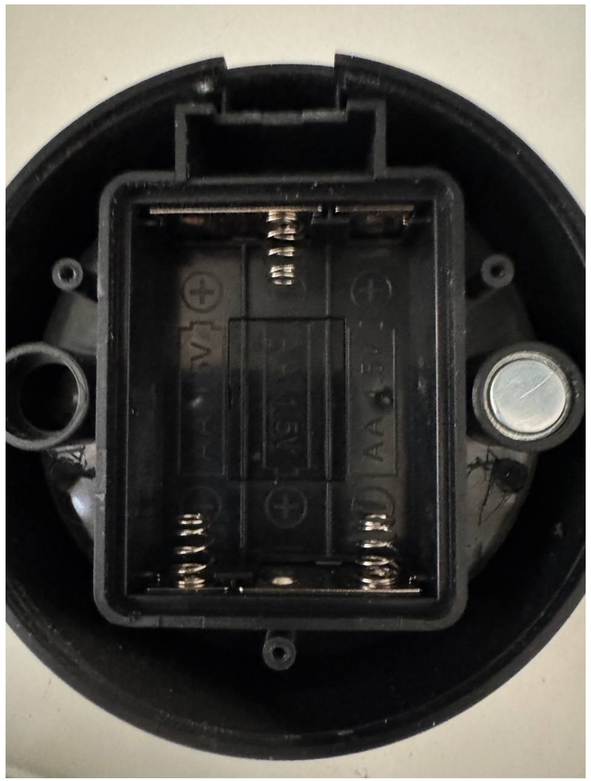
IDIADA PC25020303

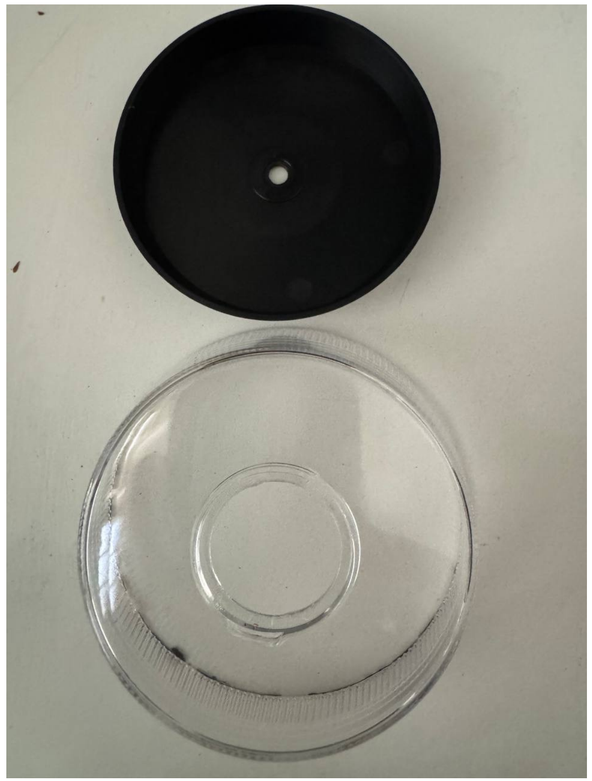
3 3 12 12 9 9 18 1 14 1 4 1 7 1 3 0

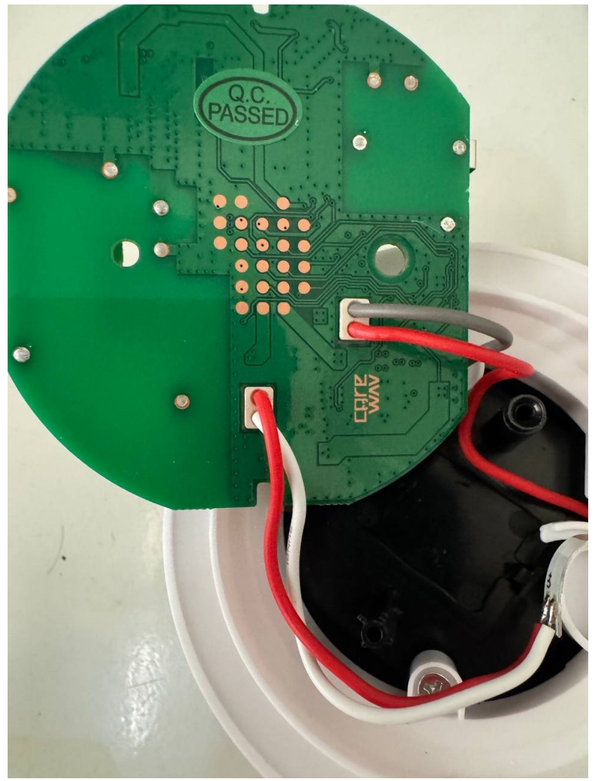
Señal V16: componentes hardware

V16 XL Perform Tools modelo 688034 – 700 candelas (Cert. IDIADA PC25020097)









Señal V16: componentes hardware

/Rooted

V16 XL Perform Tools modelo 688034 – 700 candelas (Cert. IDIADA PC25020097)





General Features

Frequency Bands: Cat-NB2
B3/B5/B8/B20/B28
Control Via AT Commands
Supply voltage range:
3.0V~4.2V [NB+GNSS]
2.2V~4.2V [NB only]
Operation temperature: -40℃ to +85℃
Dimensions: 17.6×15.7×2.4 mm
Weight: 1.2g±0.2g
GNSS(Optional): Support GPS/GLONASS/Galileo*

Data

Uplink: 159Kbps
Downlink:127Kbps

GNSS

Time-To-First Fix2:
Cold starts 29s
Hot starts <2s

Consumption

- NB only
  - 1.7uA@ PSM
  - 0.48mA @ Idle (DRX=2.56s)
  - 0.25mA @ Idle
  (eDRX=40.96s; PTW=81.92s)

Other Features

Firmware update via UART
TCP/UDP/HTTP/DNS/NTP/PING/TLS*/DTLS*
LWM2M*/COAP/MQTT
OneNET/CTWING
DFOTA

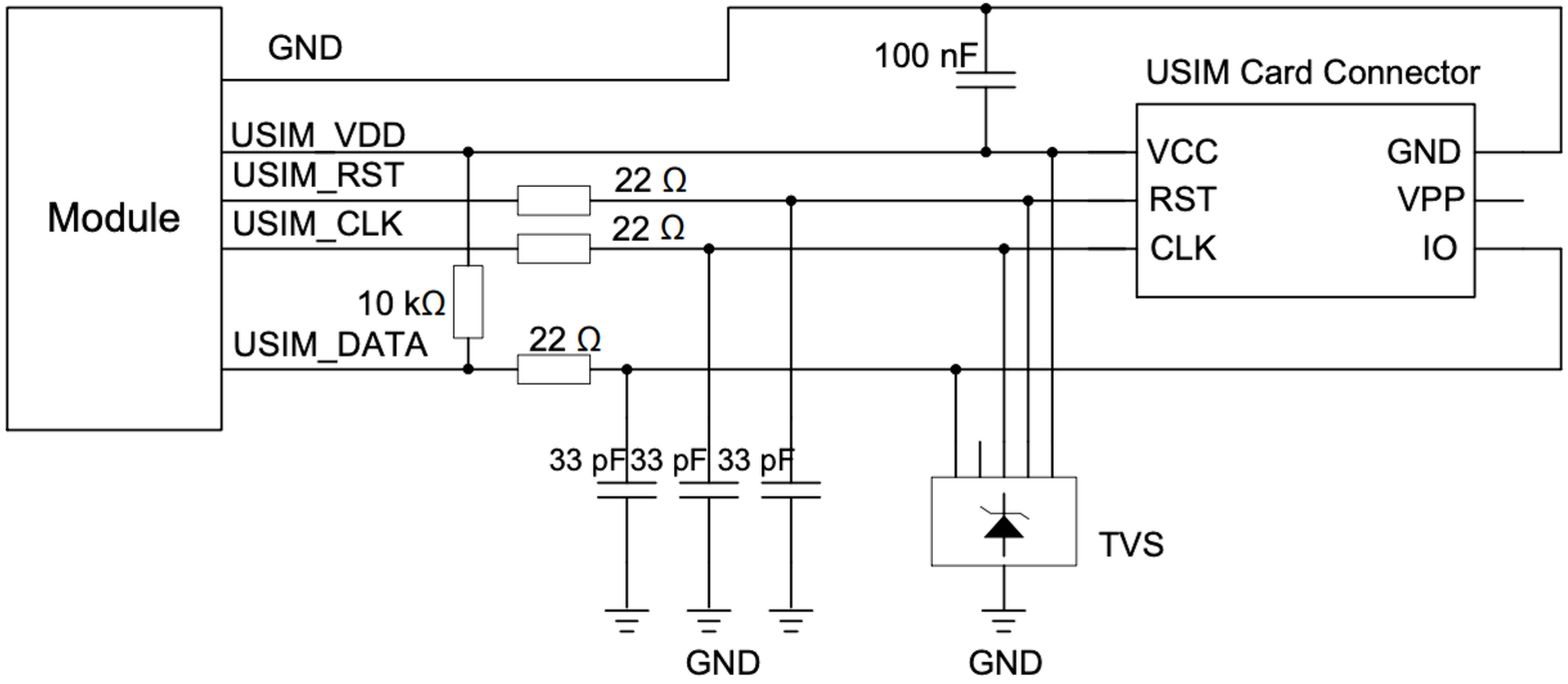
Interfaces

UART
USIM card (1.8V/3V)
Netlight
RI
ADC
GPIO

Señal V16: componentes hardware

eSIM / Embedded SIM

TP9 → USIM_VCC
TP31 → USIM_DATA
TP32 → USIM_CLK
TP33 → USIM_RST
TP34 → GND



Señal V16: componentes hardware

/Rooted

NB-IoT AT Commands

```
# Reboot the modem
at+nrb

# Query the firmware version
at+cgmr

# Get the IMSI
at+cimi

# Query the state of the radio
at+cfun?

# Turn the radio on
at+cfun=1
```

```
at+cfun?
+CFUN:1
at+cimi
51**************1

# Set the network operator PLMN, or MCCMNC
# Command returns immediately but attachment
# takes lot of time
at+cops=1,2,"xxxxx"

# Query attachment state
at+cgatt?
...
at+cgatt?
+CGATT:1
OK
```




Señal V16: componentes hardware

/Rooted

```
# Query radio statistics
at+nuestats

Signal power:-1053
Total power:-875
TX power:23
TX time:822
RX time:30289
Cell ID:27****48
DL MCS:0
UL MCS:0
DCI MCS:1
ECL:1
SNR:-64
EARFCN:3740
PCI:471

OK
```

```
# Query the PDP context
at+cgdcont?

# Check the address within the local network
at+cgpaddr

# Check the bands supported by the module
at+nband?

# Ping an external server
at+nping=8.8.8.8
```




Señal V16: componentes hardware

```
# Open
at+nsoc
0
OK


# Send
# This
at+nsos


# Open
at+nsoc


# Send
at+nsos
```



Señal V16: componentes hardware

/Rooted

GPS

```
TP12 → GPS_RESET
TP13 → GPS_TXD
TP14 → GPS_RXD      9600 baudios 81N
TP16 → GND
TP17 → VCC
```




```
$GNRMC,203544.000,A,0438.9198,N,07404.3962,W,0.00,247.85,150517,,,A*62
$GNGGA,203544.000,0438.9198,N,07404.3962,W,1,10,0.94,2597.0,M,3.4,M,,*69
...
```

Señal V16: componentes hardware

/Rooted

PCB

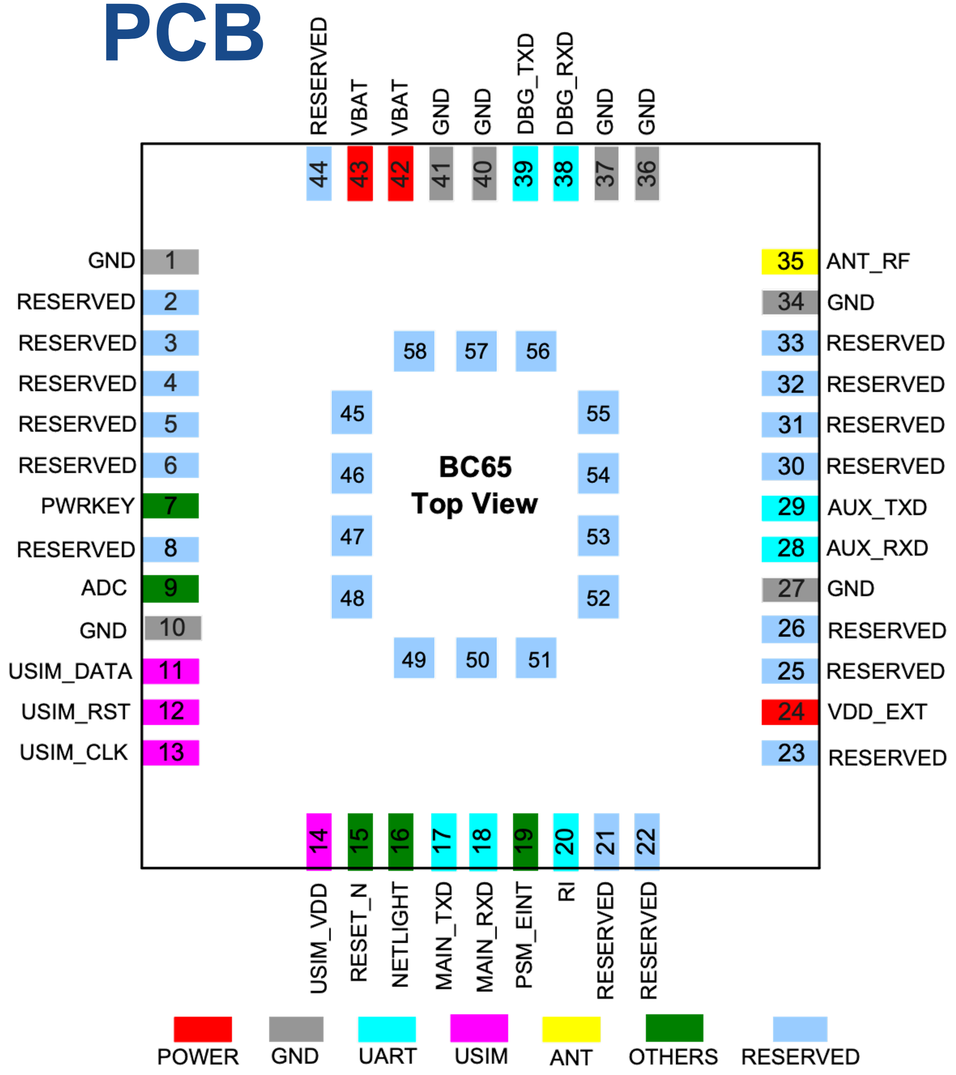




Table 12: Pin Definition of UART Interfaces

Interface	Pin Name	Pin No.	Description	Comment
Main UART	MAIN_RXD	18	Main UART receive	1.8 V power domain
	MAIN_TXD	17	Main UART transmit	
Debug UART	DBG_RXD	38	Debug UART receive	
	DBG_TXD	39	Debug UART transmit	
Auxiliary UART*	AUX_RXD	28	Auxiliary UART receive	
	AUX_TXD	29	Auxiliary UART transmit	

Señal V16: componentes hardware

PCB

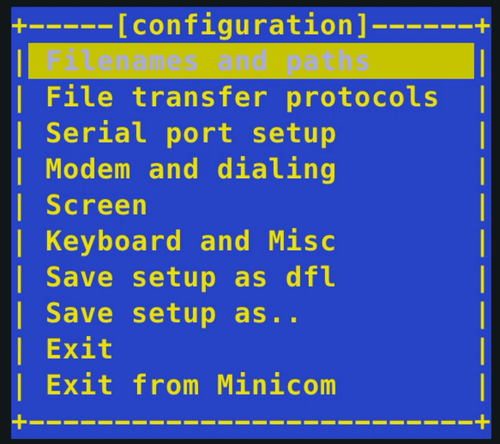
TP1 → NB_TX_DEBUG
TP2 → NB_RX_DEBUG
TP4 → NB_TXD18V
TP5 → NB_RXD18V
TP6 → NB_RESET
TP7 → NB_RXD33V
TP8 → NB_TXD33V

TP3 → GND
TP10 → VCC



Señal V16: componentes hardware

Arranque en modo DEBUG


+-----[configuration]------+
| Filenames and paths |
| File transfer protocols |
| Serial port setup |
| Modem and dialing |
| Screen |
| Keyboard and Misc |
| Save setup as dfl |
| Save setup as.. |
| Exit |
| Exit from Minicom |
+---------------------------+

Señal V16: componentes hardware

```
SendM>AT+NV=GET,VER
RecvM<2213B04Y7080E_M3EAT,Y7080E,HW_101+F241128,V1100B
10208R00C0004P07
---
SendM>AT+NCONFIG=AUTOCONNECT,FALSE
RecvM<OK
SendM>AT+NCONFIG=RELEASE_VERSION,13
RecvM<OK
SendM>AT+NCONFIG=PCO_IE_TYPE,PCO
RecvM<OK
SendM>AT+NCONFIG=RAI,FALSE
RecvM<OK
```



Señal V16: componentes hardware

```
SendATCmd(CMD_IMEI)
SendM>AT+CGSN=1
MdmPro:4.7
RecvM<+CGSN:86866108985xxxx
IMEI=86866108985xxxx
RecvM<OK
…
SendATCmd(CMD_CPIN?)
SendM>AT+CPIN?
MdmPro:4.9
RecvM<+CPIN:READY
RecvM<OK
```



Señal V16: componentes hardware

```
SendATCmd(CMD_IMSI)
SendM>AT+CIMI
MdmPro:4.11
RecvM<21407433722xxxx
IMSI=21407433722xxxx
RecvM<OK
…
SendATCmd(CMD_UDP_SEND)
SendM>AT+NSOST=0,172.31.46.162,50000,77,303737303031
303030303032333133303730303331363633433735303038
363836363130383938353236383530344532380
MdmPro:4.3
RecvM<0,77
RecvM<OK
```




GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
DGT
Dirección General de Tráfico
/Rooted
Señal V16
Ataques
V16
CONECTADA
A DGT 3.0
Obligatoria desde
01/01/26
Dispositivo que aumenta tu seguridad.
Para vehículos inmovilizados en carretera.

Ataques a la señal V16

Transmisión en texto plano vía APN de los parámetros de la baliza al fabricante sin integridad

La conexión está autenticada por el IMEI y otros datos, aunque su **transmisión no se encuentra cifrada** y es **vía UDP**

Ataque: se plantea la duda razonable si es posible autenticarse de forma anónima en el APN ofrecido.

Respuesta: sí, ***es posible con una SIM pre-autorizada por el operador***.

Ataques a la señal V16

/Rooted

Ataque: ¿Irse a una tienda donde venden las balizas, hacer una foto y **obtener varios IMEIs que han sido pre-autorizados** para su conexión y emplearlos?

Respuesta: ***no es posible***, hacen falta otros datos internos del operador como:

```
ID;CREDENTIALS;TYPE;NAME;ICCID;SHELL;com_cumulocity
_model_Agent;c8y_Mobile.imsi;c8y_Mobile.imei
123456789123456;LF2PWJOL;nbiot;Device1;12345678912
3456;;;1;{};123456789123456;98765432109876 5
```




Ataques a la señal V16

/Rooted

Ataque: **extracción de la SIM física** o de sus datos y clonación.

Respuesta: ***es posible*** y dado que el IMEI no es asociado a ningún cliente (no se piden datos de registro de la SIM), esto garantiza la anonimidad en la red del operador.

Ataque: **Man in the Middle** (**protocolo UDP**)

Respuesta: las características de este tipo de redes, las tramas de otros dispositivos ***no pueden "escucharse"*** aunque estemos autenticados ya que estos se encuentran **isolados**.



Ataques a la señal V16

Los mensajes transmitidos **no garantizan su integridad.**

Ataque: manipulación de parámetros

Respuesta: ***sí, es posible***. No se dispone de ningún mecanismo tipo H-MAC o similares para garantizar al menos su integridad, por lo que es posible inyectar cualquier texto en los campos disponibles. No obstante, es necesario tener acceso físico al dispositivo para poder realizarlo, ***ya que tiene que ser en el origen***.

Ataques a la señal V16

Fake BTS (Conexión a una estación falsa BTS)

Ataque: **suplantación de una celda de telefonía** por potencia emitida mayor en la BTS con respecto a la baliza.

Respuesta: excepto que se conozca de antemano el IMEI y otros datos, aunque se incluya para el APN el parámetro **`AT+COPS=0`** que lo conectaría automáticamente a la celda con la mejor señal, ***no es posible*** ya que se trata de una conexión autenticada.

Ataques a la señal V16

/Rooted

Su funcionamiento es simple:

- **Dispositivo y SIM**: se inserta una tarjeta SIM NB-IoT segura en el dispositivo IoT (sensor, medidor inteligente, etc.).
- **Configuración del APN**: se configura el APN (Access Point Name) proporcionado por el operador en el dispositivo.
- **Acceso a la red**: la SIM se autentica y obtiene acceso a la red NB-IoT/LTE-M (4G/5G LPWA de 3GPP), una tecnología LPWAN (Low-Power Wide-Area Network).
- **Conexión IP**: el dispositivo recibe una dirección IP para establecer la sesión de datos y transmitir información.



Ataques a la señal V16

Precisamente en el **paso 3** es **cuando no funcionaría nuestra falsa estación BTS** ya que, para dicha autenticación, es necesario tener el IMEI y otros datos de la SIM de la víctima.

- ✓ Sin embargo, ***en caso de conocerse***, si que pueden ser empleados otros ataques como DoS/Eavesdropping, Man-in-the-Middle con lectura y/o manipulación de parámetros en tiempo real, etc.

  Los APN se encuentran en los mismos hardcodeados como **balizadgt.movistar.com**, **m2mtrial.telefonica.com**, **mconnect.ot.com**, **172.31.46.149:5000**... y son comunes a todas las existentes.

Ataques a la señal V16

/Rooted

Excelente investigación de **Daniel Estévez** (EA4GPZ / M0HXM)

- ✓ **https://destevez.net/2025/12/decoding-a-v16-beacon/** (**Decoding a V16 beacon**)
- ✓ **https://destevez.net/2026/01/v16-beacon-full-uplink-conversation/** (**V16 beacon full uplink conversation**)



Ataques a la señal V16

/Rooted

Ataque: "eUICC remote provisioning" is the feature standardized by the GSMA 'SGP.02 - Remote Provisioning Architecture for Embedded UICC Technical Specification. Version 3.2'

Respuesta: dependerá del módulo y SIM empleada en la red del operador. Por ejemplo, las de Telefónica para el fabricante AMPER SISTEMAS en el producto V16 (firmware v16.1.8) para la banda 20 no lo implementan.

Se están aceptando bugs abiertos "*no bloqueantes*" en los certificados y ensayos realizados.



Ataques a la señal V16

/Rooted

Ensayo del modelo **"CarLite Geo: Baliza 3e MOD. 100"** comercializada como **3Energy-V16**

Telefónica Tech AI OF THINGS

Madrid, 3rd May 2023

To whom it may concern,

Please, be informed the **3Energy-V16** has finished IoT/M2M Device Validation process according to the data detailed in this testing report.

1. Validation result[1]

As a result of Device Validation process, Telefonica has verified that the tested device under testing, **3Energy-V16** has several non-blocking issues.

Summarizing, this document records all the issues found, and Telefonica strongly recommends solving, as soon as possible:

- "P2-High" issues 1 because they may affect the device.
- "P4-Low" issues 11 are related to those features to take into account. Telefonica's recommendation is to solve them to achieve important product improvements.

It is important to point out that:

- **Device behaviour** regarding retry scheme has the highlights reported in section 5.
- **Subscription SWAP[2]** is **NOT supported** by this version of the device under testing.

seguridad «XXUGNLWI» en: https://extranet.idiada.com/hom-cve

3 3 12 12 9 9 14 14 11 11 6 6 18 18 10 14 1 4 1 7 1 3 0

ANNEX I: Open Bugs

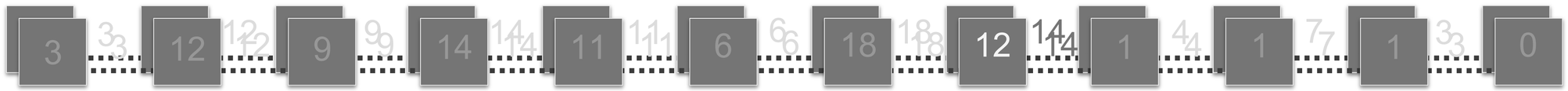
From Khepera collaborative tool:

Bug ID	Priority	Summary	High level analysis and impact
138234	P4 - Notification	[Regional] Synchronized behaviour between devices	Does the device follow 3GPP standard? **N/A** Does the device follow Telefonica requirements? **No** Impact: The device does not avoid synchronized behaviour, and does not employ a randomised pattern for signalling.
138235	P4 - Notification	Lack of support of FW upgrade method	Does the device follow 3GPP standard? **N/A** Does the device follow Telefonica requirements? **No** Impact: Lack of OTA FW upgrade method.
138237	P4 - Notification	[Regional] Application Server Down and Server IP unreacheable	Does the device follow 3GPP standard? **Yes** Does the device follow Telefonica requirements? **No (accepted by use case)** Impact: DuT has followed more retries that the ones recommended by Telefónica. However this behaviour has been accepeted
138239	P4 - Notification	[Regional] Wrong behaviour after ATTACH REJECT with cause #3 in VPLMN in 4G	Does the device follow 3GPP standard? **Yes** Does the device follow Telefonica requirements? **No (accepted by use case)** Impact: DuT has followed more retries that the ones recommended by Telefónica. However this behaviour has been accepeted
138253	P4 - Notification	[Regional] PDN CONNECTIVITY REJECT with cause #32 in 4G in HPLMN or VPLMN	Does the device follow 3GPP standard? **No** Does the device follow Telefonica requirements? **No (accepted by use case)** Impact: DuT has followed more retries that the ones recommended by Telefónica. However this behaviour has been accepeted

3 3 12 12 9 9 14 14 11 11 6 6 18 18 11 14 1 4 1 7 1 3 0

Ataques a la señal V16

Estos **quedan sin solución** en el modelo comercializado ya que el dispositivo comercializado, ***no admite actualizaciones OTA*** (otro bug admitido en el estudio realizado).



Ataques a la señal V16

GPS Spoofing (falsear la información de las señales GPS)

Ataque: generación de falsas señales GPS por un SDR.

Respuesta: está comprobado que los dispositivos ***pueden ser engañados*** para localizarse en otros puntos geográficos de donde se encuentran realmente.

Ataques a la señal V16

Jamming (GPS y cobertura móvil)

Ataque: generación de ruido para impedir la recepción de las señales de GPS y de las bandas NB-Iot/LTE-M (4G/5G LPWA de 3GPP) de telefonía empleadas (3, 5, 8, 20 y 28)

Respuesta: es relativamente sencillo realizarlo con un SDR y el dispositivo ***no sería capaz de poder recibir la señal del GPS y/o conectar a la red*** para poder transmitir las señales al fabricante.


GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
DGT
Dirección General de Tráfico
/Rooted
Baliza V16
Reversing del firmware y de una Aplicación
V16
CONECTADA
A DGT 3.0
Obligatoria desde
01/01/26
Dispositivo que aumenta tu seguridad.
Para vehículos inmovilizados en carretera.

Ingeniería inversa (Reversing)

/Rooted

The „terrible“ 3 cent microcontroller



MCU	PTB150CSE	PMS150C-S08	BJ8P509F	PFS154-S08	MDT10P509(A)	HR7P153P45SA	PFS173-S08	HT68F001
Manufacturer	**Puolop** China www.puolop.com	**Padauk** Taiwan www.padauk.com.tw	**Bojuxing Industrial** China www.bjxmcu.com	**Padauk** Taiwan www.padauk.com.tw	**Yspring Tech / MDT** China www.yspringtech.com	**Eastsoft Micro** China www.essemi.com	**Padauk** Taiwan www.padauk.com.tw	**Holtek** Taiwan www.holtek.com
Package	SOP8-150mil	SOP8-150mil	SOP8-150mil	SOP8-150mil	SOP8-150mil	SOP8-150mil	SOP8-150mil	SOP8-150mil
Price (100pc)	0.0315 USD/pc	0.0334 USD/pc	0.0466 USD/pc	0.0692 USD/pc	0.0795 USD/pc	0.0811 USD/pc	0.0859 USD/pc	0.0875 USD/pc
CPU Architecture	PDK13 79 Instructions Stack in RAM Single cycle Interrupts: Yes	PDK13 79 Instructions Stack in RAM Single cycle Interrupts: Yes	BJ13 (PIC) 42 Instructions 5 level HW stack Single cycle? Interrupts: Yes	PDK14 82 Instructions Stack in RAM Single cycle Interrupts: Yes	PIC12 36 Instructions 2 level HW stack 4 clocks/instr. Interrupts: No	HR7P RISC 79 Instructions 8 level HW stack 2 clocks/instr.? Interrupts: Yes	PDK15 88 Instructions Stack in RAM Single cycle Interrupts: Yes	Holtek12 (PIC12) 63 Instructions 2 level HW stack 4 clocks/instr. Interrupts: Yes
ROM	1k x 13 bit OTP	1k x 13 bit OTP	1k x 13 bit OTP	2k x 14 bit Flash	1k x 12 bit OTP	2k x 16 bit OTP	3k x 15 bit Flash	0.5k x 12 bit Flash
RAM	64 Bytes	64 Bytes	49 Bytes	128 Bytes	41 Bytes	64 Bytes	256 Bytes	16 Bytes
Periphery	6 GPIO 16 bit timer 1x8 bit timer/PWM Analog comparator Brownout reset Watchdog timer	6 GPIO 16 bit timer 1x8 bit timer/PWM Analog comparator Brownout reset Watchdog timer	6 GPIO 1x8 bit timer Brownout reset Watchdog timer	6 GPIO 16 bit timer 2x8 bit timer/PWM 3x11 bit PWM Analog comparator Brownout reset Watchdog timer	6 GPIO 1x8 bit timer Brownout reset Watchdog timer	6 GPIO 2x8 bit timer/PWM 1x12bit ADC Brownout reset Watchdog timer	6 GPIO 16 bit timer 2x8 bit timer/PWM 3x11 bit PWM Analog comparator 1x8bit ADC Brownout reset Watchdog timer	6 GPIO 1x8 bit timer Brownout reset Watchdog timer
Clock	16 MHz internal 62 kHz internal	16 MHz internal 62 kHz internal	8 MHz internal External RC External XTAL	16 MHz internal 70 kHz internal External XTAL	8 MHz internal	16 MHz internal 36 kHz internal External XTAL	16 MHz internal 93 kHz internal External XTAL	- 32 kHz internal External XTAL
Programming	4+2 wire HV (12V)	4+2 wire HV (12V)	?	3+2 wire HV (8V)	?	3+2 wire HV (8.5V)	3+2 wire HV (8V)	2+2 wire ICP
Vendor IDE	?	Padauk Dev. Studio (ASM, Mini-C)	Bojuxing IDE (ASM)	Padauk Dev. Studio (ASM, Mini-C)	MDT-IDE, Yspring writer	?	Padauk Dev. Studio (ASM, Mini-C)	Holtek HT-IDE3000 (ASM)
OSS Toolchain	Tentative, SDCC >=3.9.0	Tentative, SDCC >=3.9.0	No	Yes, SDCC >=3.9.0	Yes, GPUTILS (PIC tools)	No	Yes, SDCC >=3.9.0	No
Notes	Website and datasheet in Chinese		Website in chinese, but english datasheet		PIC12C509 clone, horrible datasheet	Website and datasheet in chinese		Ultra low power

https://cpldcpu.wordpress.com/2019/08/12/the-terrible-3-cent-mcu/

Ingeniería inversa (Reversing)

/Rooted

soporte.incidence.eu/hc/es

Please enable cookies.

Error 1034

Ray ID: 9d09d9f61f06cbb7 • 2026-02-20 00:22:45 UTC

Edge IP Restricted

What happened?

You've requested a page on a website that is part of the Cloudflare network. The host (soporte.incidence.eu) resolved to an IP address that the owner of the website does not have access to.

What can I do?

If you are a visitor of this website:
Please try again in a few minutes.

If you are the owner of this website:
Check your DNS records to ensure they are pointed to the IP address you were assigned at registration.

Was this page helpful? Yes No
Thank you for your feedback!

Cloudflare Ray ID: **9d09d9f61f06cbb7** • Your IP: Click to reveal [redacted] • Performance & security by Cloudflare

DEMO

3 3 12 12 9 9 14 14 11 11 6 6 18 18 14 14 2 4 1 7 1 3 0

Java decompiler online / APK

decompiler.com

Incógnito

Decompiler.com JAR String Editor Release Notes support@decompiler.com

Drop EXE or DLL,
JAR or CLASS,
APK, XAPK or DEX,
PYC or PYO,
LUAC or LUB,
SMX or AMXX file here
Choose file

Fast AI apps start with fast data. Get low-latency data with Redis Cloud. **Try for free now.**

Ads by EthicalAds



Upload your artifact

Drag and drop your artifact into the online decompiler to view the content online or download it.



All online

Navigate through and inspect decompiled code online without installing anything.



F#, Visual Basic, C# decompiler

.exe and .dll .NET decompilation back to C# project.



Java decompiler

.jar and .class decompilation back to Java source code.



Android decompiler

.apk, .xapk and .dex decompilation back to Java source code.



Python decompiler

.pyc and .pyo decompilation back to Python source code.



Lua decompiler

.luac and .lub decompilation back to Lua source code.

/Rooted

Java decompiler online / APK

decompiler.com

Incógnito

Decompiler.com JAR String Editor Release Notes support@decompiler.com

Drop EXE or DLL,
JAR or CLASS,
APK, XAPK or DEX,
PYC or PYO,
LUAC or LUB,
SMX or AMXX file here
Choose file

Augment Code Review Beats Copilot, Cursor & Claude on Code Review **Install Now**

Ads by EthicalAds



Upload your artifact

Drag and drop your artifact into the online decompiler to view the content online or download it.



All online

Navigate through and inspect decompiled code online without installing anything.



F#, Visual Basic, C# decompiler

.exe and .dll .NET decompilation back to C# project.



Java decompiler

.jar and .class decompilation back to Java source code.



Android decompiler

.apk, .xapk and .dex decompilation back to Java source code.



Python decompiler

.pyc and .pyo decompilation back to Python source code.



Lua decompiler

.luac and .lub decompilation back to Lua source code.

/Rooted


GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
DGT
Dirección General de Tráfico
/Rooted
Plataforma DGT 3.0
Explotación de los datos recopilados
V16
CONECTADA A DGT 3.0
Obligatoria desde
01/01/26
Dispositivo que aumenta tu seguridad.
Para vehículos inmovilizados en carretera.

Explotación de los datos recopilados

La plataforma DGT 3.0 es el **punto de intercambio de datos** de la Dirección General de Tráfico. Su misión: que todos los actores de la movilidad (vehículos, navegadores, apps, grúas, señalización...) **hablen el mismo idioma** y **compartan avisos verificados** en tiempo real.

- ✓ Serán datos **recibidos en todo caso** (no existe integridad del mensaje ni garantía del origen del evento).
- ✓ Frecuencia variable de actualización (pocos minutos) pero **no es en tiempo real**.

Explotación de los datos recopilados

Por la **Directiva 2010/40/EU**, podemos hacerlo de **forma pública** para los ***conjuntos de datos disponibles*** por nombre, etiqueta y organización (incluso utilizando un buscador) o suscribirnos a dichos conjuntos para mantenerse informado de los últimos cambios y actividad reciente.

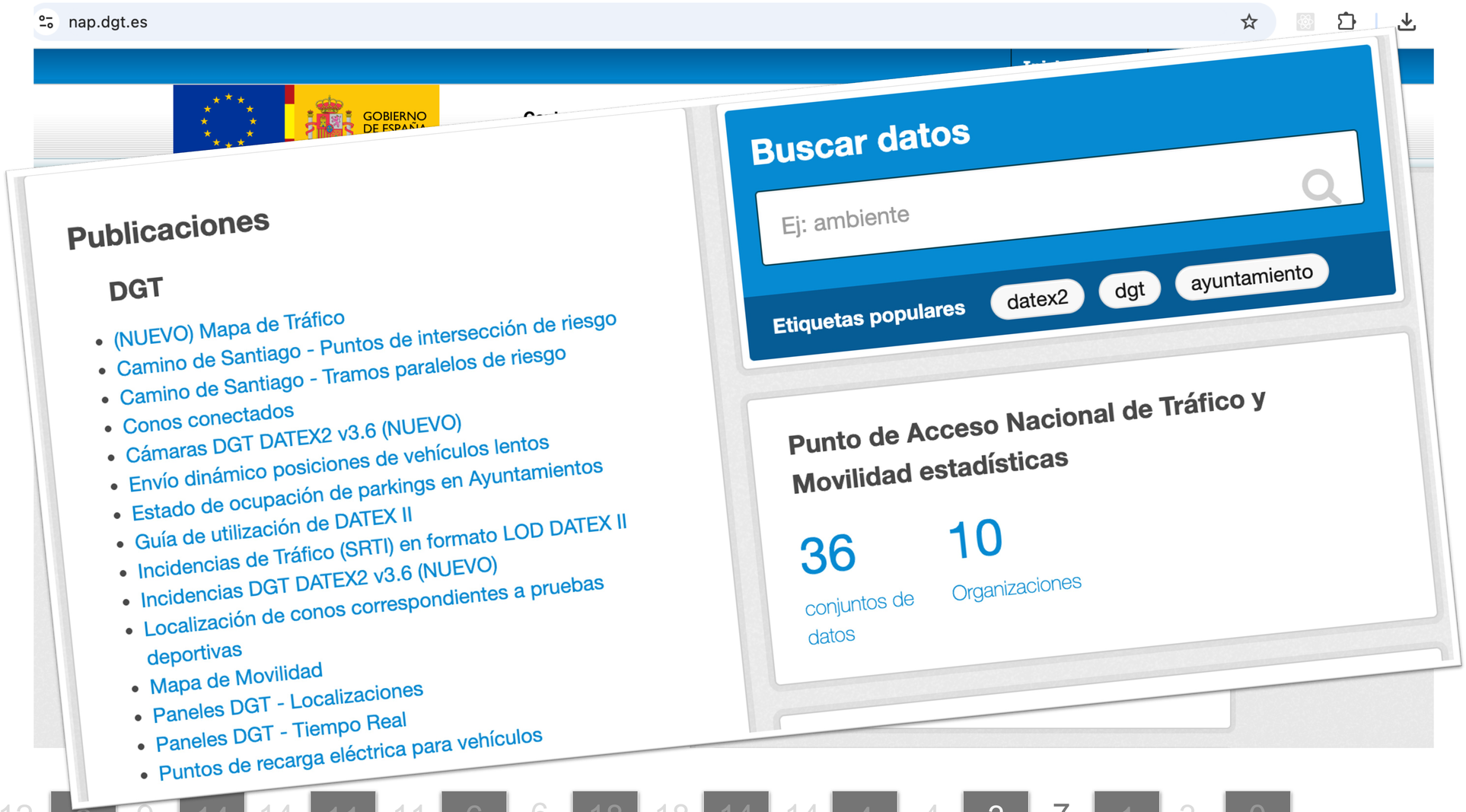
- Actualmente se dispone de **36 conjuntos** (antes 41) y **10 organizaciones**.

- Se emplea el **formato común** de datos **DATEX II** (https://nap.dgt.es/dataset/guia-de-utilizacion-de-datex-ii) por HTTPS en formato XML.

Explotación de los datos recopilados

/Rooted

Todo ello, podemos realizarlo desde https://nap.dgt.es/



Explotación de los datos recopilados

/Rooted

infocar.dgt.es/datex2/dgt/SituationPublication/paneles/content.xml

```
▼<_0:groupOfLocations xsi:type="_0:GroupOfLocationsByReference">
 ▼<_0:locationContainedInGroup xsi:type="_0:LocationByReference">
    <_0:predefinedLocationReference>GUID_PMV_60107</_0:predefinedLocationReference>
  </_0:locationContainedInGroup>
  <_0:predefinedLocationSetReference>GUID_Inventario_Pmvs</_0:predefinedLocationSetReference>
 </_0:groupOfLocations>
 <_0:datexPictogram>maximumSpeedLimit</_0:datexPictogram>
 <_0:datexPictogram>blankVoid</_0:datexPictogram>
 <_0:pictogramList>Intercentros</_0:pictogramList>
 <_0:pictogramListEntry>R301120</_0:pictogramListEntry>
 <_0:pictogramListEntry>0</_0:pictogramListEntry>
 <_0:vmsIdentifier>2</_0:vmsIdentifier>
 <_0:vmsLegend>VELOCITAT/CONTROLADA/ PER RADAR</_0:vmsLegend>
 </_0:situationRecord>
</_0:situation>
▼<_0:situation id="GUID_PMV__M_607_0015_448_C_T01">
 ▼<_0:headerInformation>
    <_0:confidentiality>noRestriction</_0:confidentiality>
    <_0:informationStatus>real</_0:informationStatus>
  </_0:headerInformation>
 ▼<_0:situationRecord id="GUID_PMV__M_607_0015_448_C_T01_1" xsi:type="_0:VariableMessageSignSetting">
```

3 3 12 12 9 9 14 14 11 11 6 6 18 18 14 14 4 4 4 7 1 3 0

Explotación de los datos recopilados

/Rooted

<_0:pictogramListEntry>R301120</_0:pictogramListEntry> → Icono señal oficial R-301-120 de "Prohibición



Explotación de los datos recopilados

A fe… **para la**
baliz… de datos
abier… su uso
(esp…

- ht…
- ht…
- ht…

nap.dgt.es/datex2/v3/dgt/SituationPublication/datex2_v36.xml


```xml
</sit:situation>
▼<sit:situation id="16729553">
 ▼<sit:headerInformation>
    <com:informationStatus>real</com:informationStatus>
  </sit:headerInformation>
 ▼<sit:situationRecord xsi:type="sit:GenericSituationRecord" id="20605295" version="1">
    <sit:situationRecordCreationReference>D30_fecff6aa-850a-4b99-a61f-8d1038de13c1_1</sit:situationRecordCreationReference>
    <sit:situationRecordCreationTime>2026-02-16T09:21:34.000+01:00</sit:situationRecordCreationTime>
    <sit:situationRecordVersionTime>2026-02-16T09:21:34.000+01:00</sit:situationRecordVersionTime>
    <sit:probabilityOfOccurrence>certain</sit:probabilityOfOccurrence>
  ▼<sit:source>
     <com:sourceIdentification>DGT3.0</com:sourceIdentification>
   </sit:source>
  ▼<sit:validity>
     <com:validityStatus>active</com:validityStatus>
   ▼<com:validityTimeSpecification>
      <com:overallStartTime>2026-02-16T09:21:34.000+01:00</com:overallStartTime>
     </com:validityTimeSpecification>
   </sit:validity>
  ▼<sit:cause>
     <sit:causeType>vehicleObstruction</sit:causeType>
   ▼<sit:detailedCauseType>
      <sit:vehicleObstructionType>vehicleStuck</sit:vehicleObstructionType>
     </sit:detailedCauseType>
   </sit:cause>
  ▼<sit:locationReference xsi:type="loc:PointLocation">
   ▼<loc:supplementaryPositionalDescription>
    ▼<loc:roadInformation>
       <loc:roadName>N-332</loc:roadName>
      </loc:roadInformation>
     </loc:supplementaryPositionalDescription>
    ▼<loc:tpegPointLocation xsi:type="loc:TpegSimplePoint">
      <loc:tpegDirection>northEastBound</loc:tpegDirection>
      <loc:tpegSimplePointLocationType>nonLinkedPoint</loc:tpegSimplePointLocationType>
     ▼<loc:point xsi:type="loc:TpegNonJunctionPoint">
      ▼<loc:pointCoordinates>
         <loc:latitude>38.016205</loc:latitude>
         <loc:longitude>-0.66024</loc:longitude>
       </loc:pointCoordinates>
      ▼<loc:_tpegNonJunctionPointExtension>
       ▼<loc:extendedTpegNonJunctionPoint>
          <lse:autonomousCommunity>Comunitat Valenciana</lse:autonomousCommunity>
          <lse:kilometerPoint>62.558</lse:kilometerPoint>
          <lse:municipality>Torrevieja</lse:municipality>
          <lse:province>Alacant/Alicante</lse:province>
         </loc:extendedTpegNonJunctionPoint>
       </loc:_tpegNonJunctionPointExtension>
```

Explotación de los datos recopilados

/Rootəd

Simplif

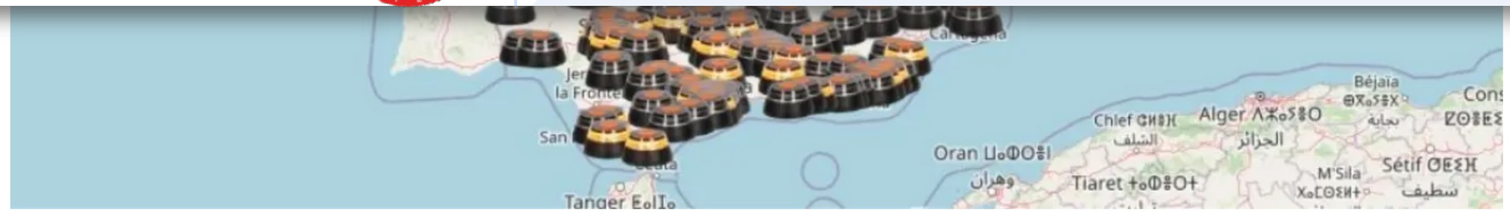
20minutos.es/motor/actualidad/hector-julian-joven-detras-mapa-balizas-v16-descubri-datos-todas-balizas-son-publicos_6925808_0.amp.html

Página | Espacio de trabajo | Anulaciones | index-CJv76Gxv.js | leaflet-D4S3Ouxg.js

- etrafficWEB
  - assets
    - css
    - js
      - i18n-Dmb49fx3.js
      - index-CJv76Gxv.js
      - leaflet-D4S3Ouxg.js
      - react-DvgQm5cF.js
      - ui-lF0upmgG.js
    - etrafficWEB/
- React Developer Tools

```
        }
        return m.notifyOnChangeProps ? v : m.trackResult(v)
    }, e, Ol)
}
function Bl(e, n="K") {
    const i = a.charCodeAt(0)
        t = atob(e)
        r = new Uint8Array(t.length);
    for (let o = 0; o < t.length; o++)
        r[o] = t.charCodeAt(o) ^ i;
    return new TextDecoder("utf-8").decode(r)
}
const ql = e => {
    try {
        return e.map(e => {
            let a;
```

DEMO



Héctor Julián, el joven estudiante de ingeniería creador del mapa de balizas V16. / Canva/mapa de balizas.

ACTUALIDAD NOTICIA 03 feb 2026 - 15:11


GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
DGT
Dirección General de Tráfico
/Rooted
Conclusiones
V16
CONECTADA
A DGT 3.0
Obligatoria desde
01/01/26
Dispositivo que aumenta tu seguridad.
Para vehículos inmovilizados en carretera.

Conclusiones

En un mundo interconectado, estos datos, siempre que **sean anónimos** y **no permitan el rastreo permanente** de los ciudadanos, pueden servirnos ***para evitar accidentes adoptando las medidas oportunas para seguir realizando una conducción segura***, estando informados en todo momento, casi en tiempo real y **sin envío de datos personales**.

En vez de la imposición legal y dadas las características que hemos visto, **se pueden aprovechar otros mecanismos para realizar la misma función** evitando "sangrar una vez más al ciudadano".

Conclusiones

Por último, existen aplicaciones que **vinculan esta señal V16 a aseguradoras y otro tipo de empresas**, para además dar un aviso automático en caso de incidente a los servicios de emergencia (eCall) y a la asistencia en carretera concertada.

Otros permiten registrarla y luego, cuando la baliza se conecte al servidor del fabricante, se recibe un **SMS** o **Whatsapp** en los teléfonos designados indicando la geolocalización o no de la misma.

Estos **sí que piden datos personales** y es **responsabilidad del fabricante** disponer de las medidas técnicas y organizativas.

¿Preguntas?



Muchas gracias

Especialmente a aquell@s que han soportado al autor durante la investigación y a:

☠️ GC3 ☠️
☠️ L1k0rd3b3ll0t4 ☠️
☠️ HuertollanoCON ☠️
☠️ P4x0Rs ☠️
☠️ Original CCC ☠️
☠️ ...etc... ☠️

/Rooted®