

Telefonica



IoT - Big Data & Security

MWC Smart Cities Seminar

Telefónica Global IoT Group
Feb 2017

IoT Big Data and IoT Security in Smart Cities



IoT
Big Data

IoT
Security

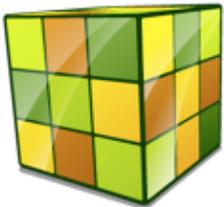
TEF IoT-Big Data Smart City Pillars



Open and horizontal platforms



A rich and dynamic ecosystem



API and data model harmonization

Open and horizontal platforms



Rely on Open Source Software

FIWARE OSS Community / FIWARE Foundation



Openness to avoid vendor lock in

Benefits mobile operators & cities :

Can choose from a variety of IoT providers, integrators, etc.



Modular and extensible architectures

No more silos of isolated, single-vertical solutions.

Enabling a real **IoT BigData Ecosystem** for smart cities.

Rich and dynamic ecosystem

Cities

Open and Agile Smart Cities Alliance (OASC).
> 100 cities.



Entrepreneurs

FIWARE Acceleration
Wayra



IoT Device Vendors

FIWARE IoT Ready Programme
> 50 kind of devices certified



Mobile Operators

Harmonization

Ecosystem + Open Platforms + **Harmonization** = Smart City Replicability

API Harmonization

Providing a single, generic RESTful API to get access to smart city data (real time or historic)
FIWARE NGSIv2

Data Model Harmonization

Defining a catalogue of harmonized data models that cover different smart city verticals

Standardization

With GSMA, our work has been aligned with 5 top operators around the world
New ETSI ISG CIM Group

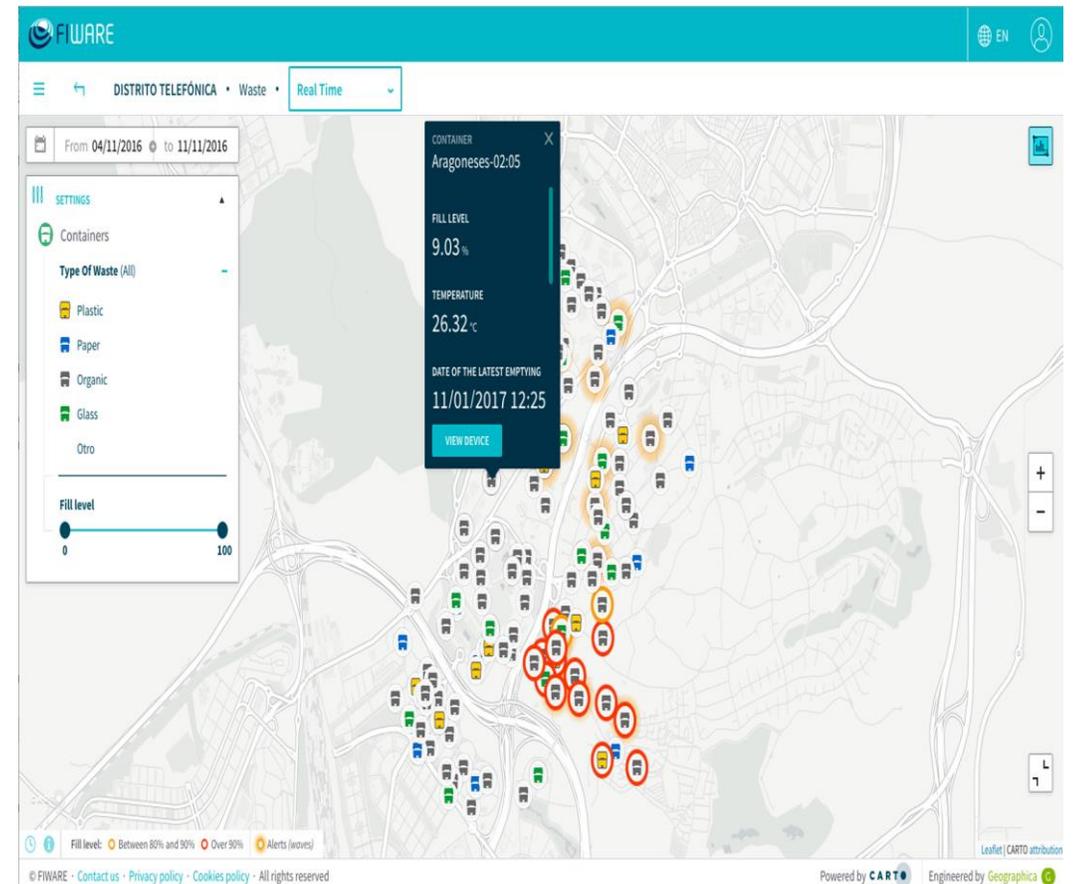


<http://www.gsma.com/newsroom/press-release/gsma-launches-iot-big-data-directory-support-growth-innovative-new-iot-solutions/>
<http://apidirectory.connectedliving.gsma.com>

Applications



Smart Car Navigator



Portable City Dashboard (URBO)

Security in Smart Cities

Personal data privacy is key

Cities infrastructure must be secure

Secure from design makes a difference



Smart cities, attack targets or attack tools?



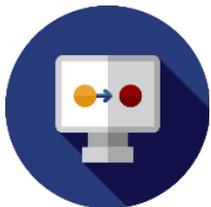
24x7 Availability, the city never sleeps



Huge number of devices



Insecure design in some assets



Low or difficult maintenance

IoT Security challenges

Heterogeneity

No one size fits
all solutions



Resources

Constrained
devices



Identity

Authentication
first



Operation

Device
management



IoT security challenges require E2E approach



- GSMA Guidelines
- Managed Connectivity
- Private APN & VPN
- Network Auth & PKI

- Comms Monitoring
- Expense controls
- Persistent Pentesting
- Threat detection

- Anti DDoS
- Managed Connectivity
- Automatic rules

IoT Security Self-Assessment in Smart Cities



GSMA IoT Security Self-Assessment helps Smart Cities across their lifecycle

Design



A guidance in the in order to assess risks, decide the prevention measures.

Deployment



A checklist to validate the security measures that has been put in place

Onlife



A standard way to exchange security information in a common language.



Carlos Carazo
Global IoT Platforms & Technology Director
carlos.carazocepedano@telefonica.com