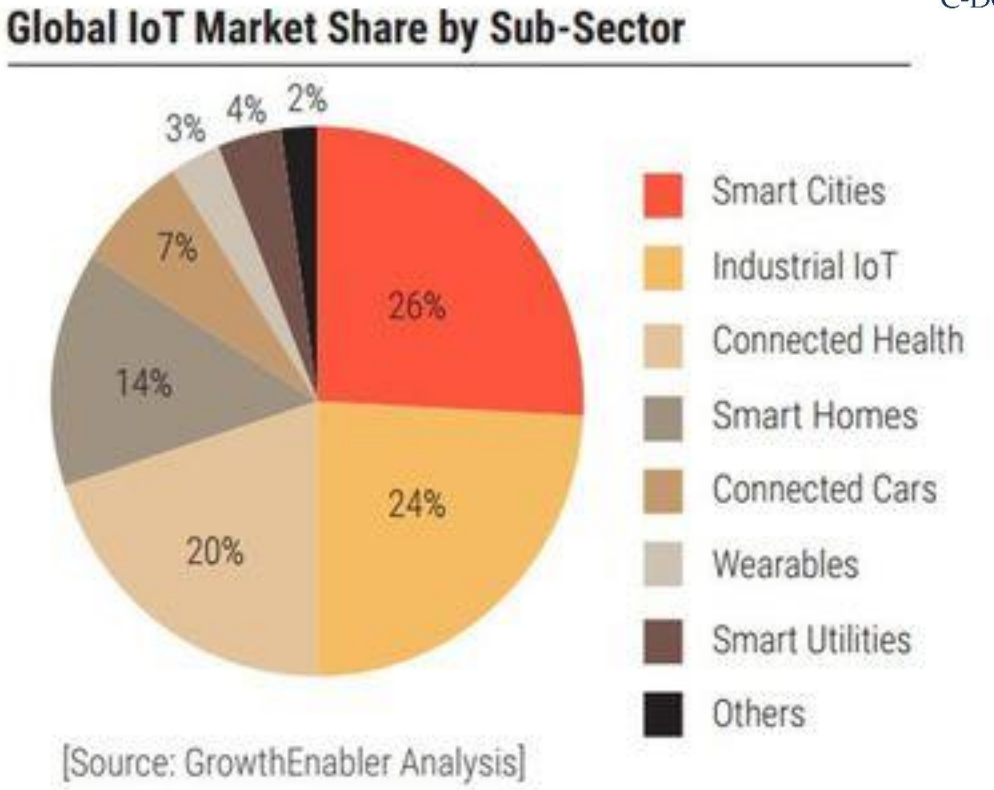
Why oneM2M is essential for India

Centre for Development of Telematics

www.cdot.in

Forecast about Global IoT Market Share

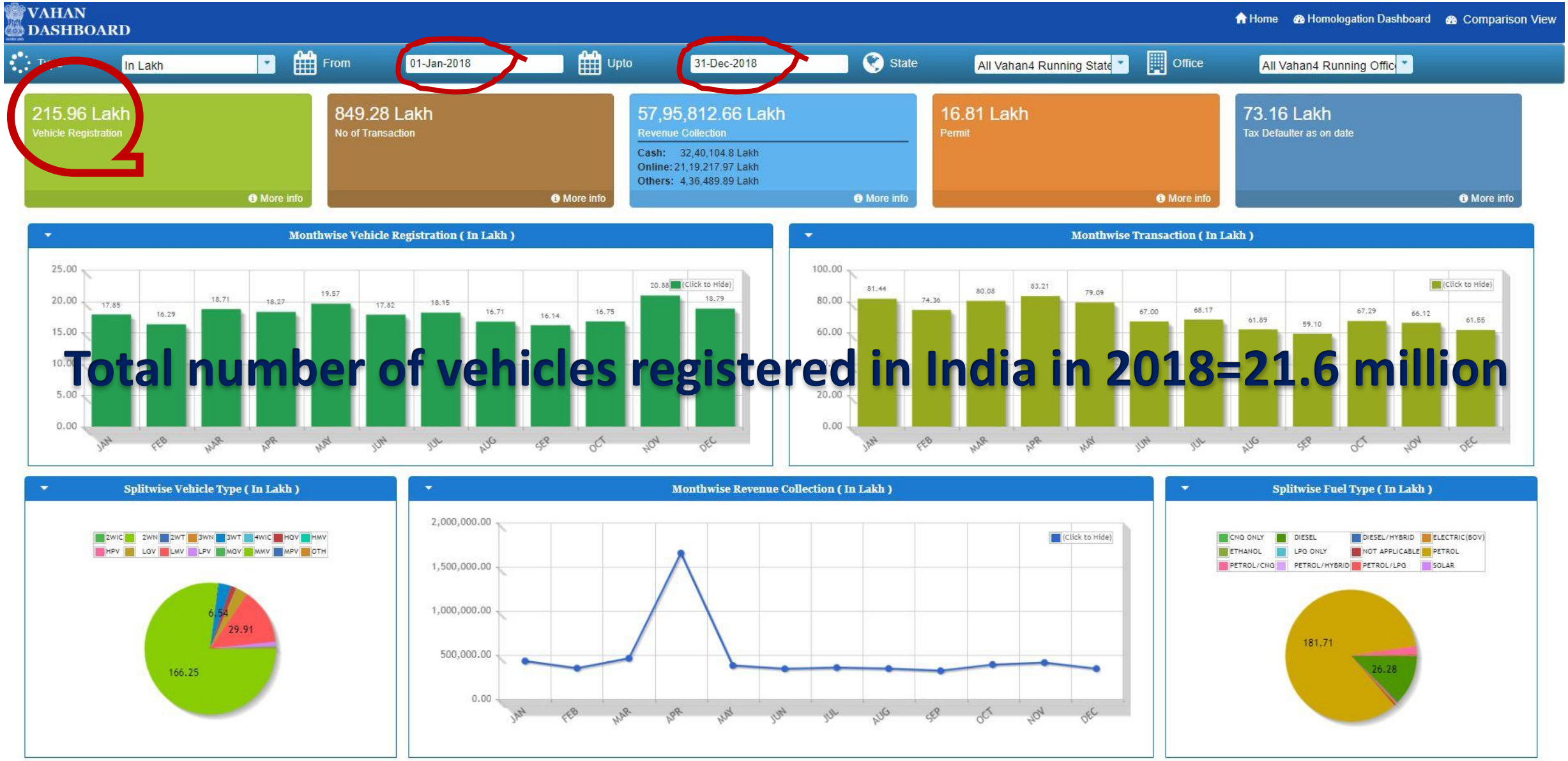
[Sources: GrowthEnabler Analysis/MarketsandMarkets]



[Source: GrowthEnabler Analysis]

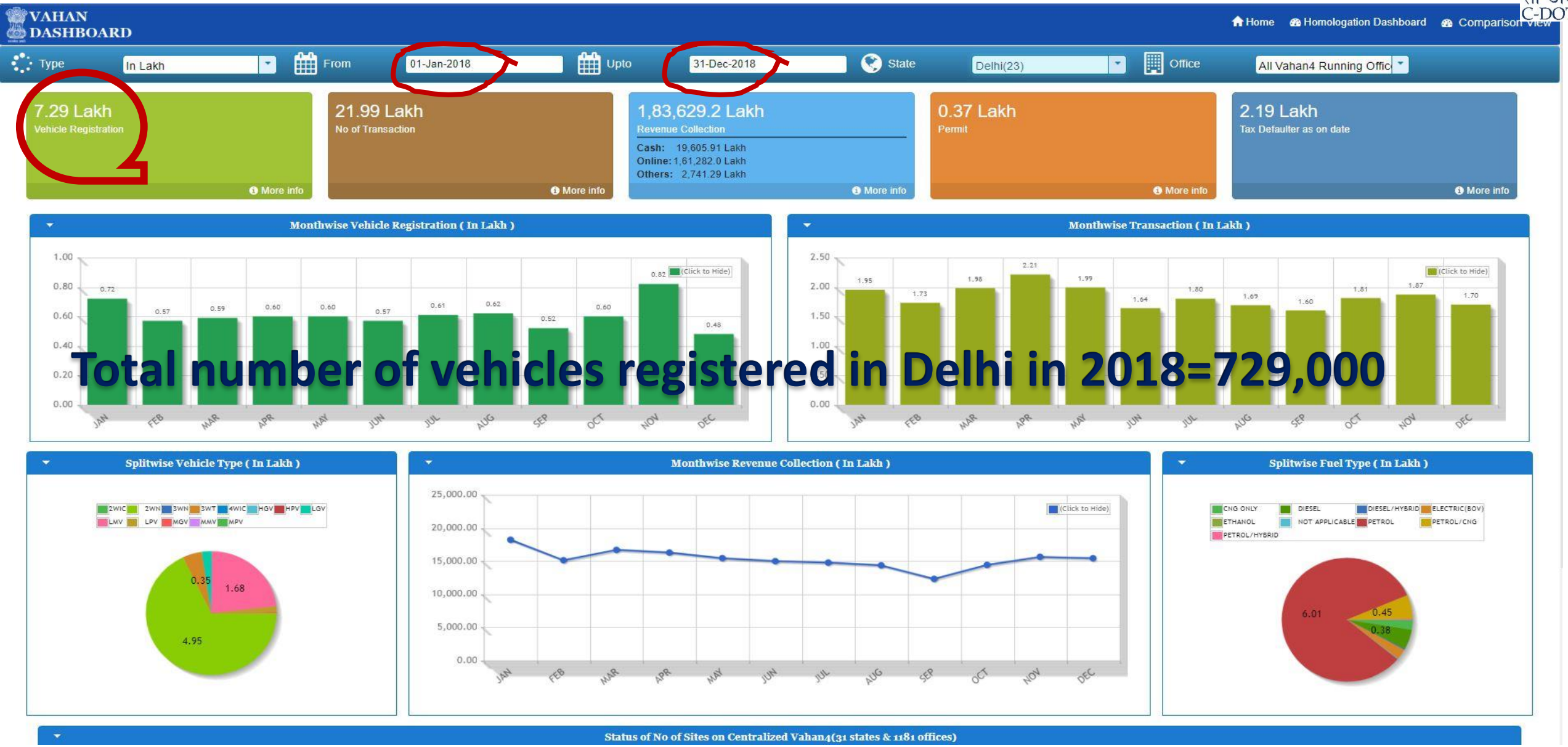
According to GrowthEnabler Report "The global IoT market will grow to $457B by 2020, attaining a Compound Annual Growth Rate (CAGR) of 28.5%. According to GrowthEnabler & MarketsandMarkets analysis, the global IoT market share will be dominated by three sub-sectors; Smart Cities (26%), Industrial IoT (24%) and Connected Health (20%). Followed by Smart Homes (14%), Connected Cars (7%), Smart Utilities (4%) and Wearables (3%)."

How it differs when we look at Geographies like India



Total number of vehicles registered in India in 2018=21.6 million

The India Aspect - Continues



Total number of vehicles registered in Delhi in 2018=729,000

The Above Figures were only showing the increment in one year

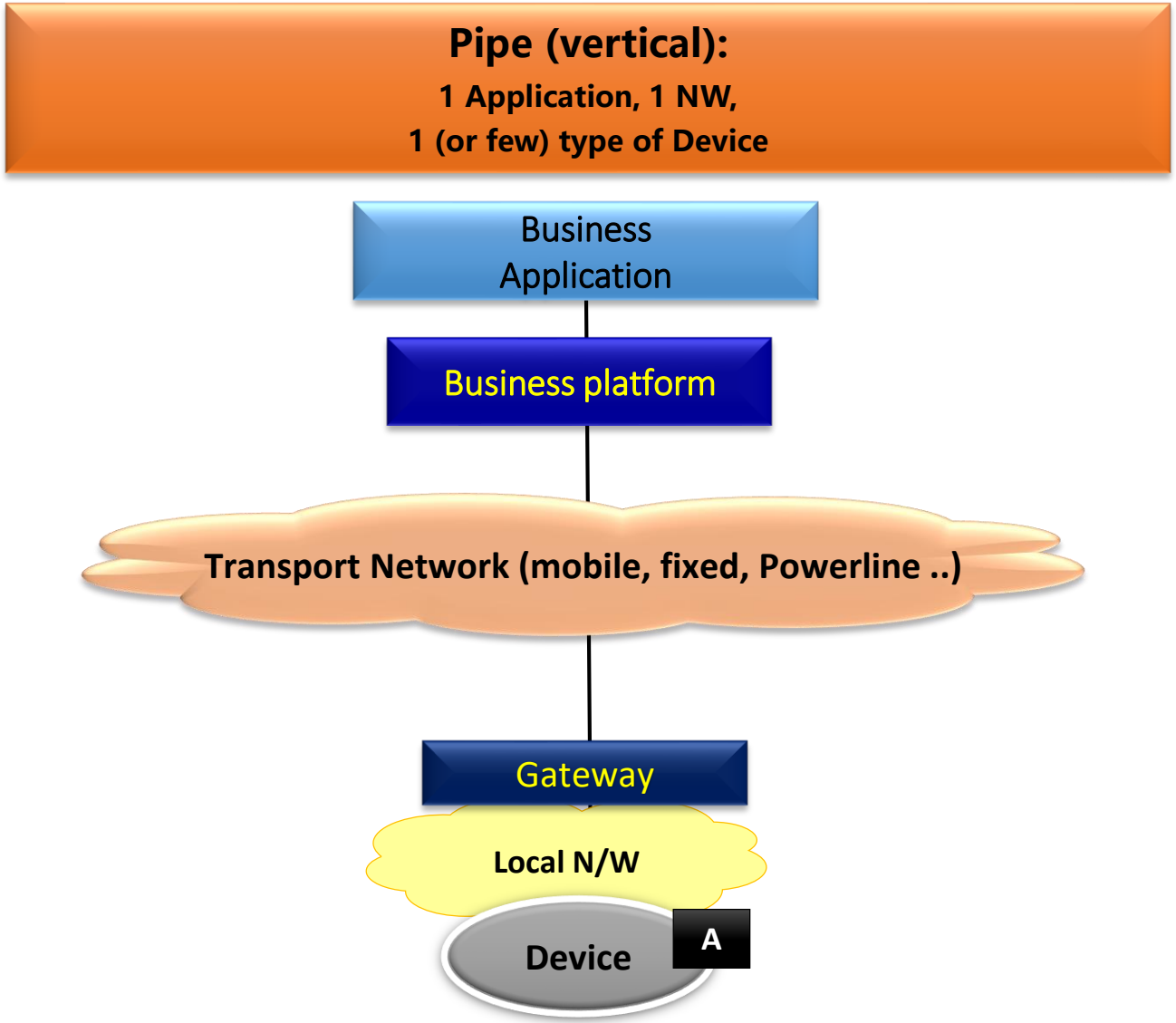
Table 1: New passenger cars by type of engine fuel, 2017

	Total	Petrol	Diesel	Alternative energy
Belgium	553,692	288,484	259,790	5,418
Bulgaria	240,121	:	:	:
Czechia	269,622	:	:	:
Denmark	221,476	142,607	77,495	:
Germany	3,441,262	1,986,488	1,336,776	143,474
Latvia	17,064	9,488	7,446	130
Lithuania	161,115	47,486	110,328	3,301
Luxembourg	52,775	:		:
Hungary	271,720	148,139	113,161	10,420
Malta	18,729	11,766	6,865	98
Netherlands	414,309	331,609	72,267	10,433
Austria	353,320	171,862	175,590	5,868
Poland	1,336,787	719,727	500,112	116,948
Portugal	224,029	78,675	139,106	6,248
Romania	627,743	199,463	422,731	5,549
Slovenia	72,477	38,229	32,410	1,838
Slovakia	165,652	:	:	:
Finland	118,587	81,435	36,216	936
Sweden	392,717	191,048	192,191	9,477
United Kingdom (²)	2,509,330	1,446,500	1,049,086	13,744
Liechtenstein (¹)	1,984	951	985	48
Norway	183,728	95,077	46,970	41,681
Switzerland	315,000	195,200	114,100	5,700
North Macedonia	26,609	:	:	:
Turkey	741,902	259,325	457,069	25,508

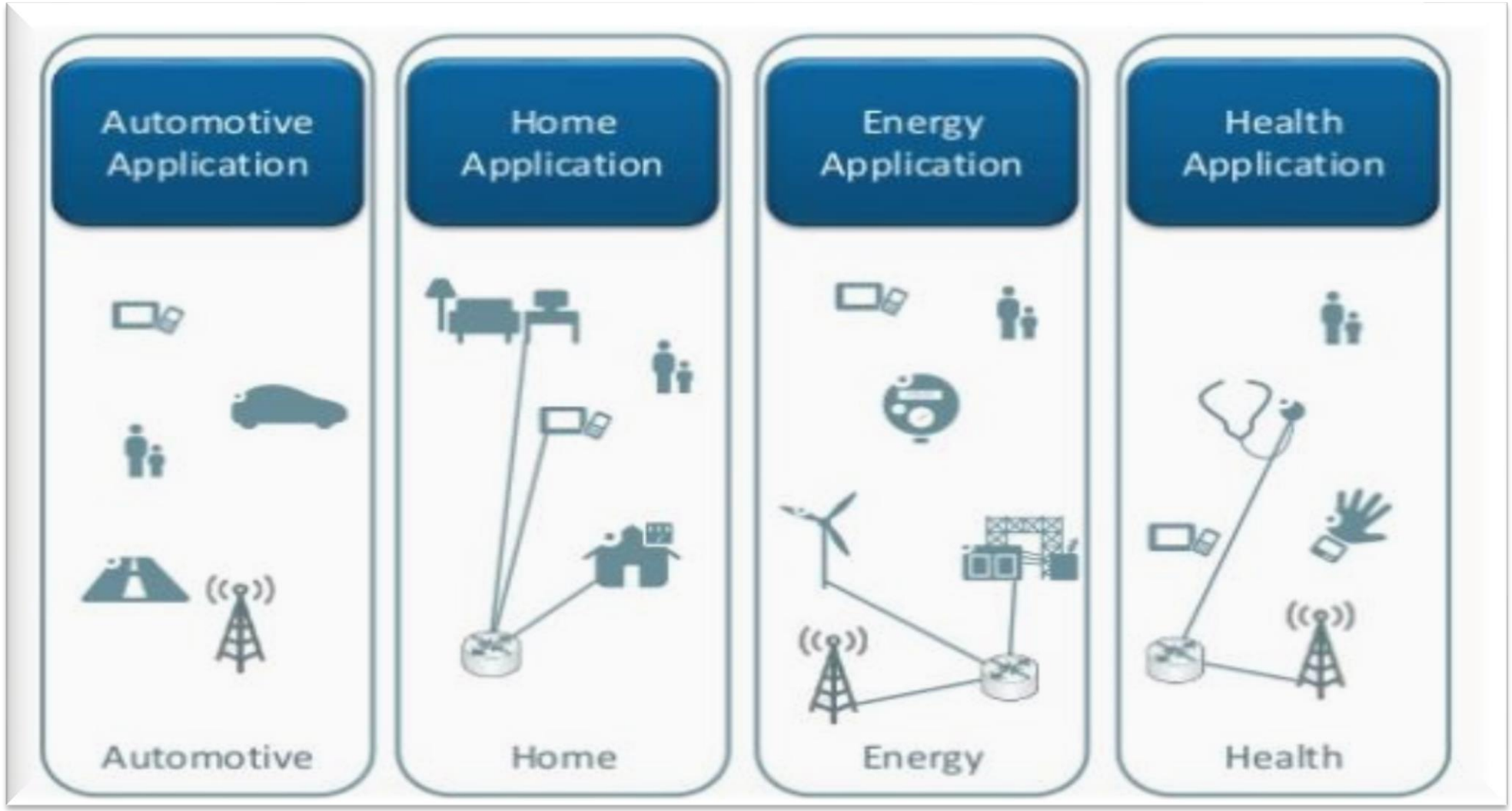
Total No. of Vehicles added in 2017 in entire Europe :

18,566,398 ≈18.6 million

Present Landscape of IoT/M2M Architecture



Current Landscape of IoT Applications in Smart City



Other City Services and Departments

vertical Centric Siloed Ecosystem

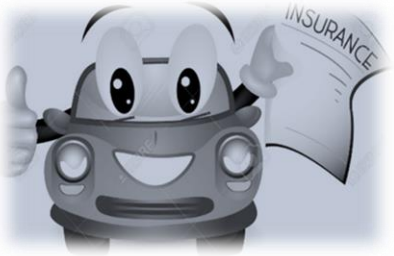
Issues Plaguing the IoT/M2M Ecosystem

- Security- Device Security, Authentication, Communication Security, Data Integrity, Data Privacy, Lawful Interception. IoT also brings existential threat to mankind unlike Cyber Security which affects monetarily
- Interoperability(or lack of it): Due to non-standardised proprietary implementations the devices and applications do not interoperate; giving rise to vendor lock-in and therefore higher TCO
- No Sharing of Data: Sharing of data amongst divergent applications is a key requirement for IoT/M2M Deployments. Non-standardised proprietary implementations make it extremely difficult.
- Device Ownership: Ownership of the devices communicating, KYC
- Spectrum Availability
- Addressability: limited address space for mobile devices(10 digit, 13 digit or more..), IPv6?
- Power Supply(long Battery life, energy harvesting..), Software Complexity, Semantics, Self-management And Self-healing of IoT/M2M devices and Regulatory Aspects (licensing, Service Provider Registration etc.)

Data Sharing Example

- Cars fitted with various sensors send information to the manufacturer

- The service provider servicing the car may also need access some to the sensor data



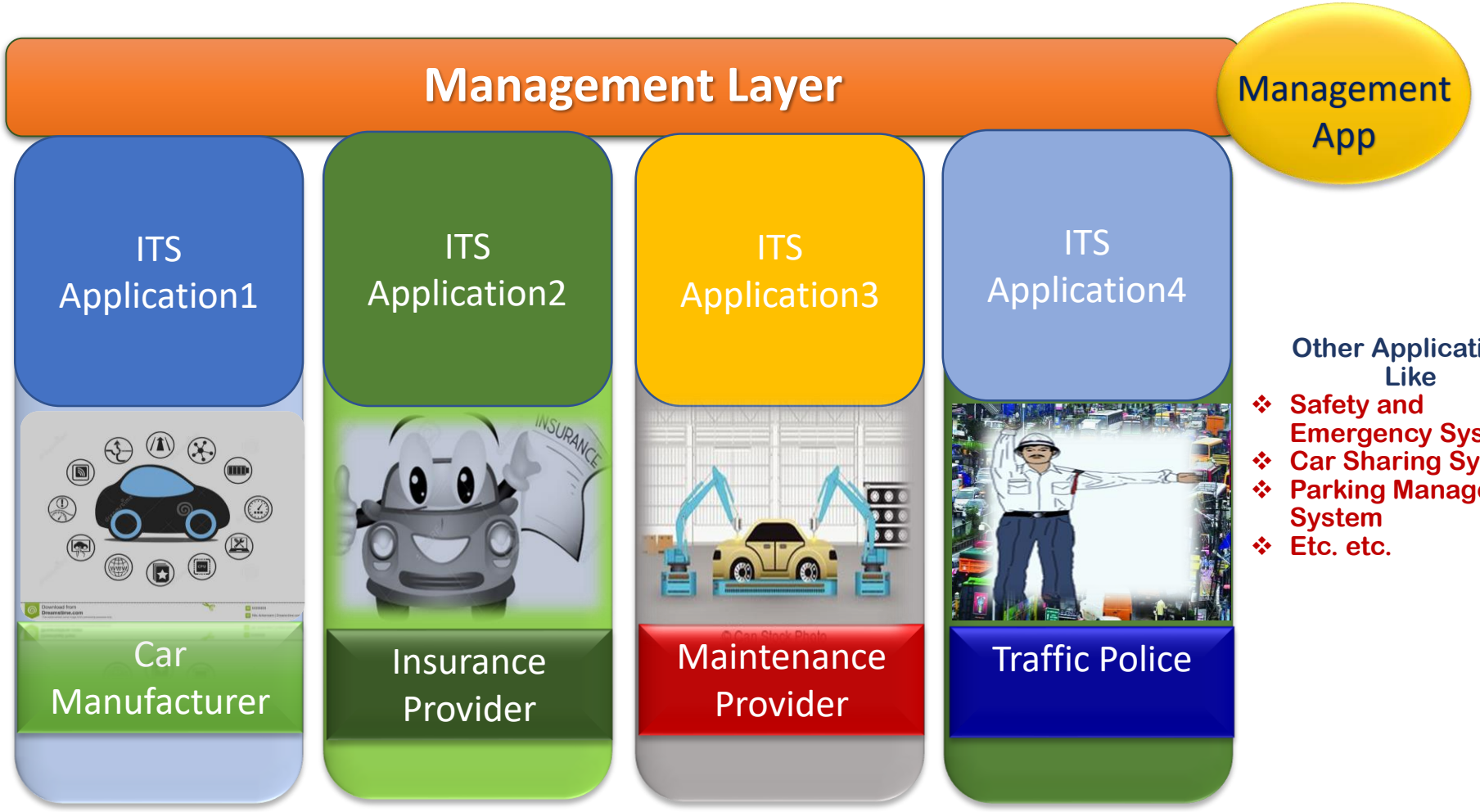
- The insurance company providing insurance for the car also needs information as to how the car is driven and based on this info charges the premium. The fraudulent insurance claims would also be minimised.

- The on-road assistance company would require the location information of the car to send appropriate assistance

- The traffic police would like to know accident information to be able to manage traffic.

- This information would be useful for the commuters to select alternate route

Current State of Vertical Centric Siloed Ecosystem



Other Applications Like

- Safety and Emergency Systems
- Car Sharing System
- Parking Management System
- Etc. etc.

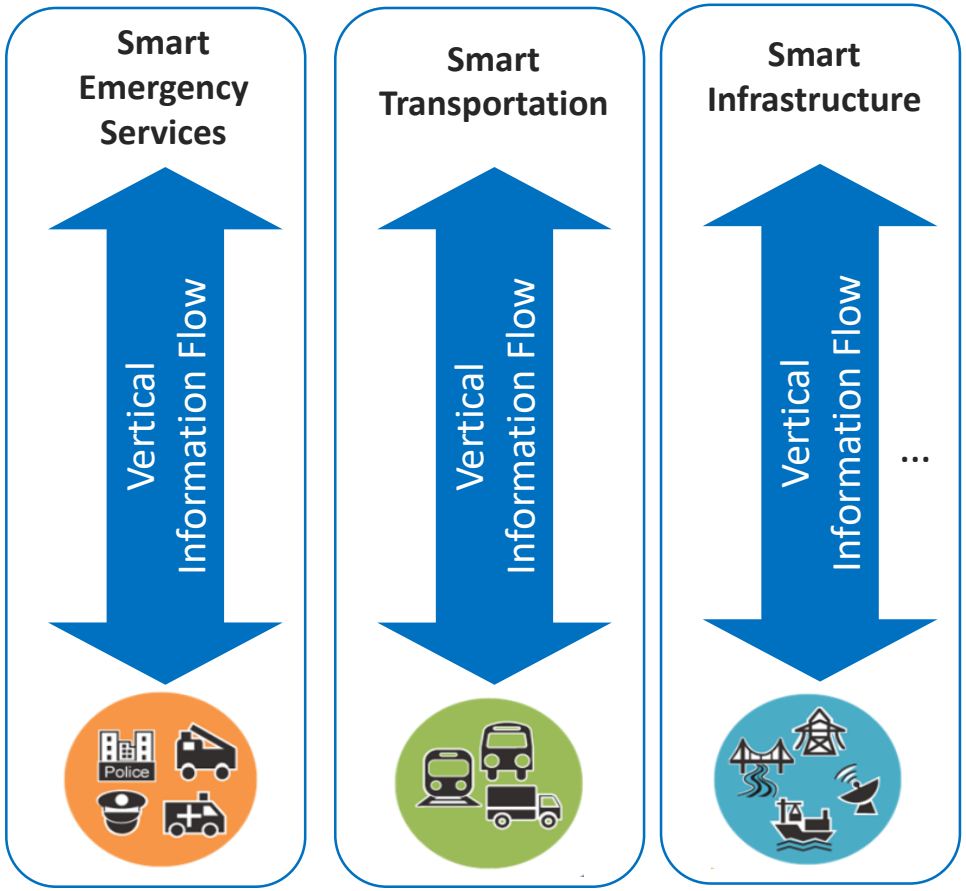
IN ORDER TO SHARE DATA AMONG ALL THESE SILOED (PROPRIETARY) APPLICATIONS ANOTHER LAYER WOULD HAVE TO BE CREATED WHICH CAN EXTRACT DATA FROM THESE APPLICATIONS

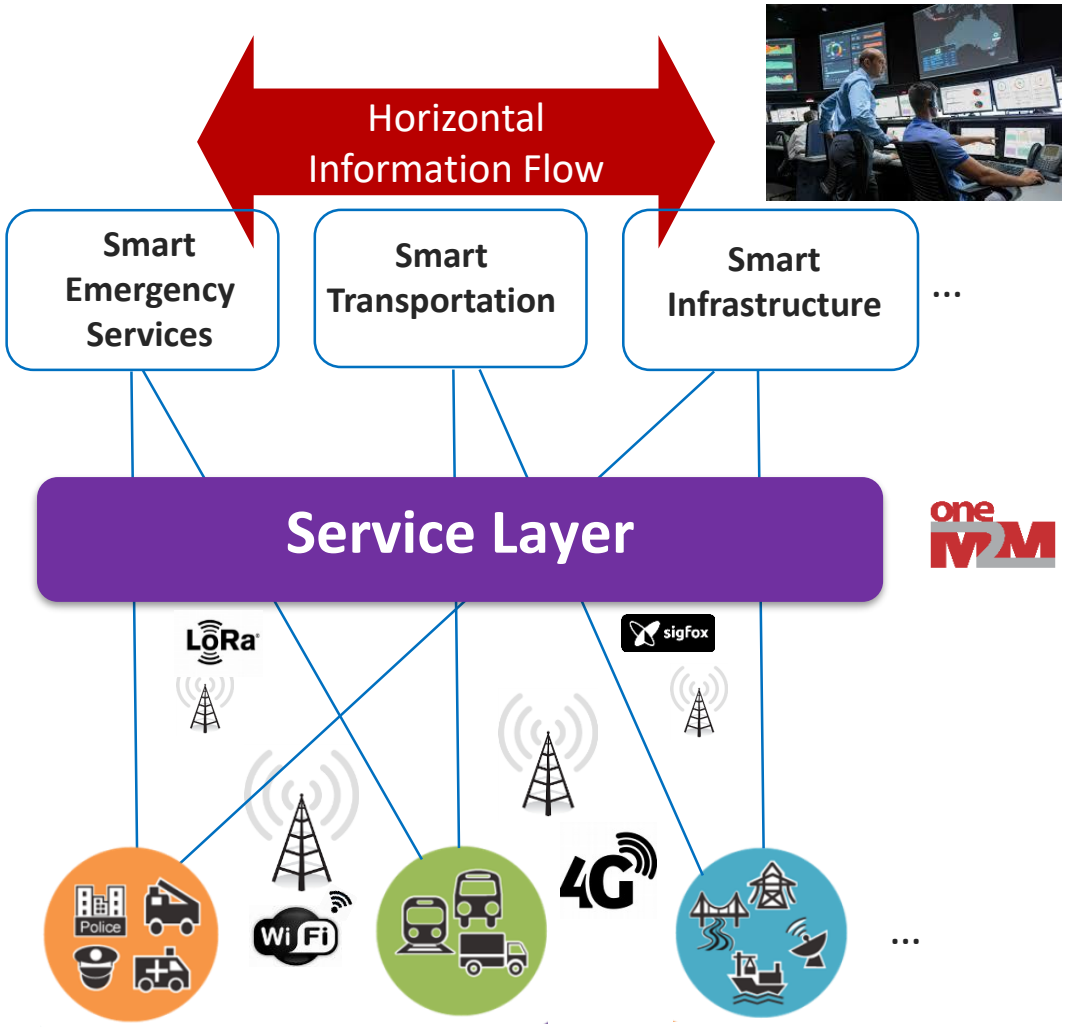
Q. What's the Solution?

A. Standardised Common Service Layer

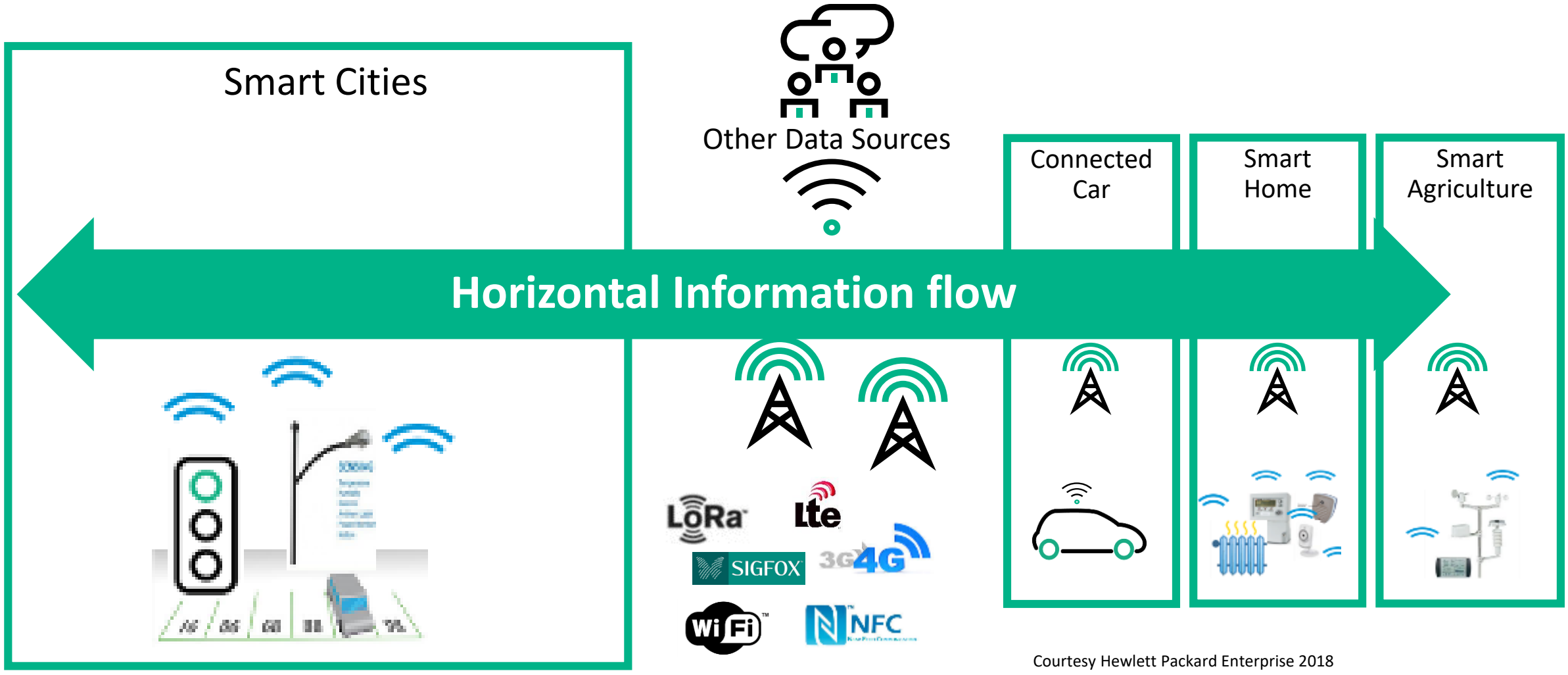
i. e.

oneM2M Breaks Down the Silos



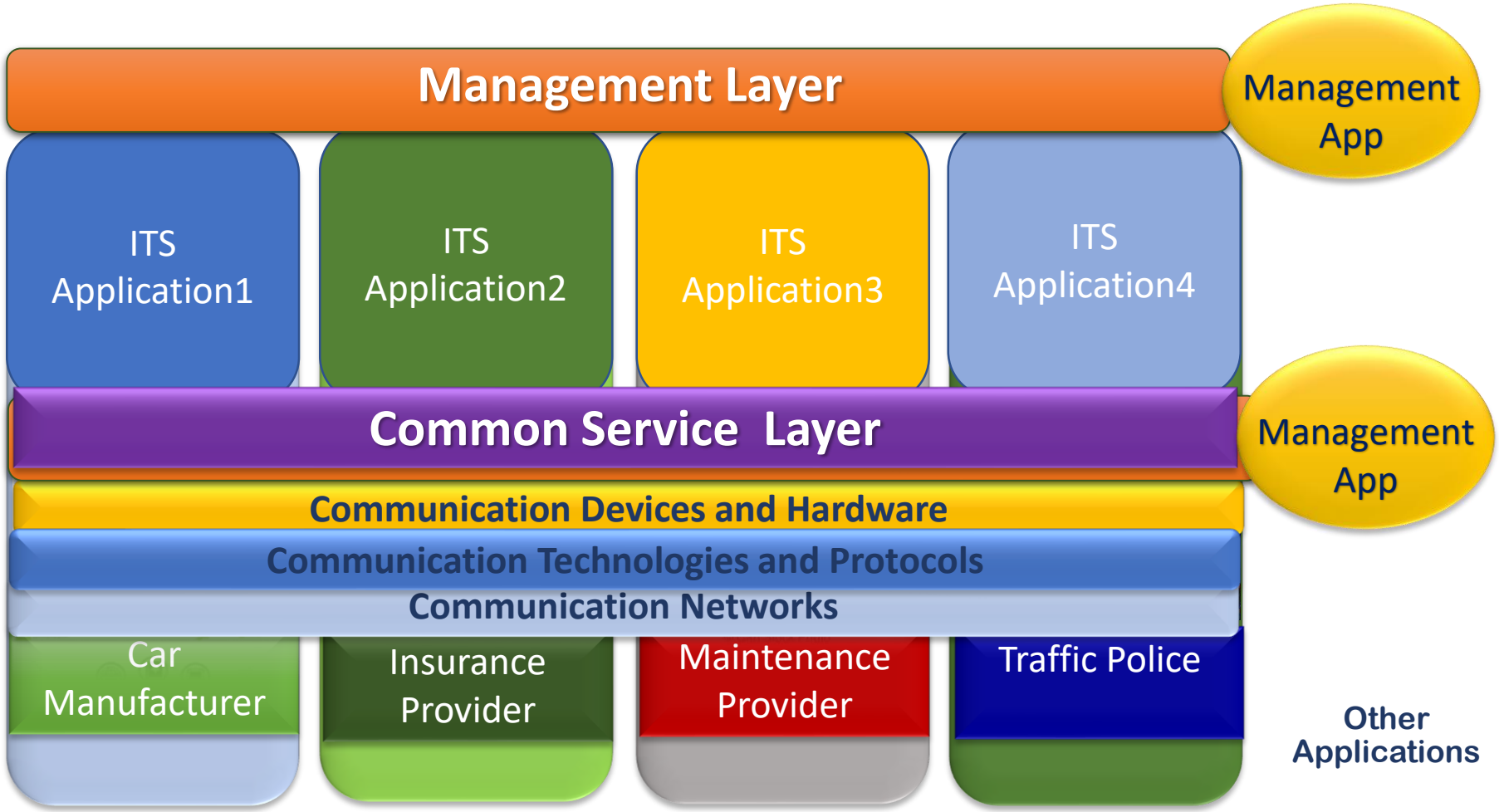


Need for horizontal IoT platform connecting the ”things”



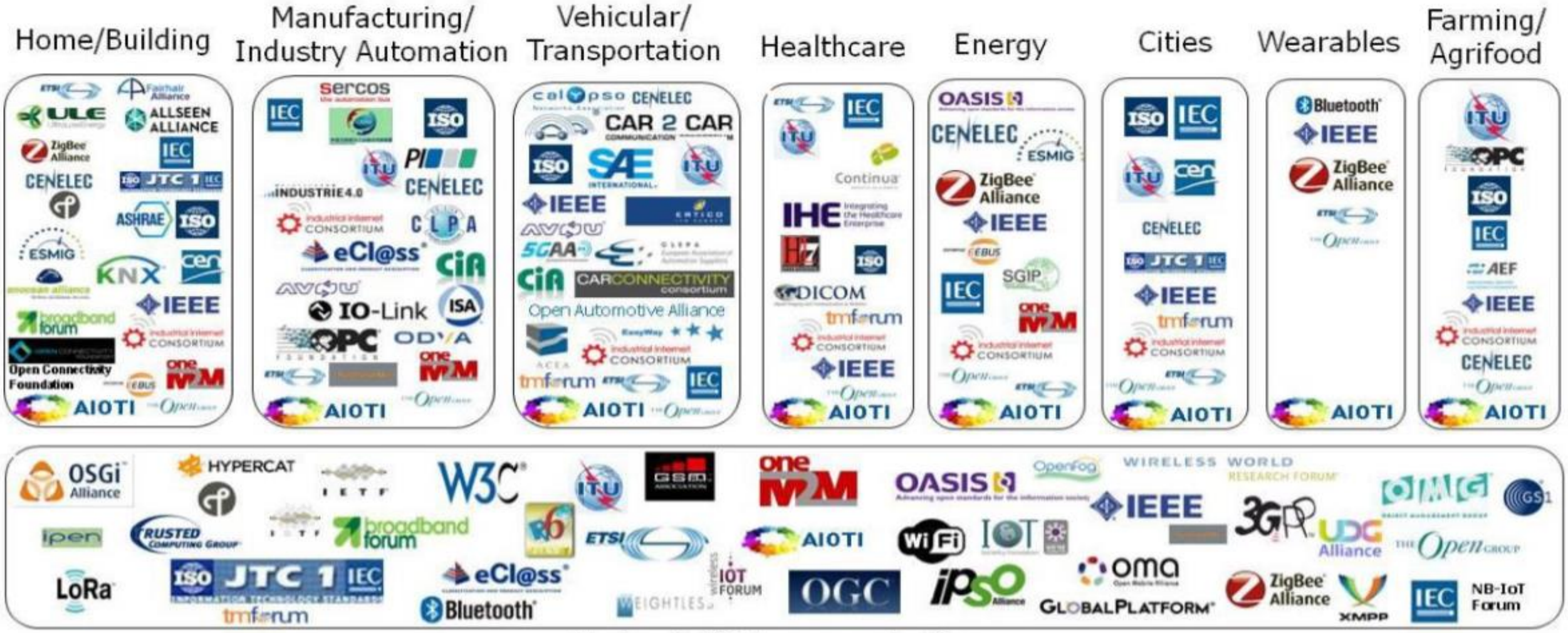
Courtesy Hewlett Packard Enterprise 2018

Horizontal Approach of oneM2M for the IoT Applications



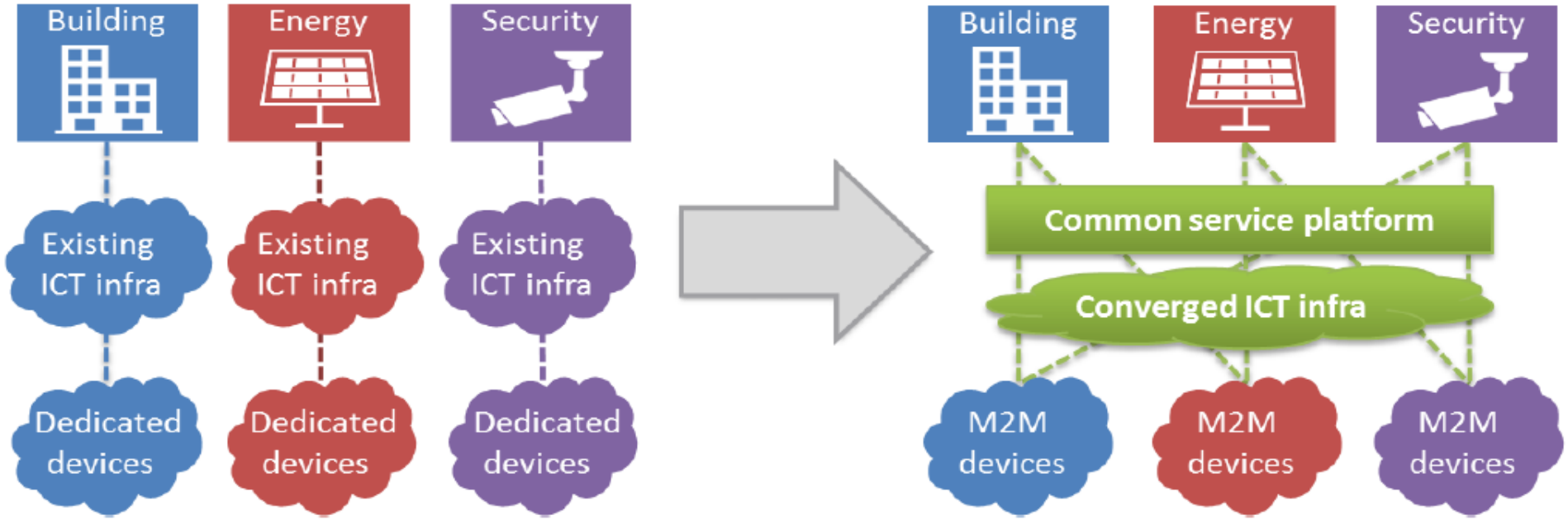
The Standardised Common Service Layer, being and integral part of the IoT/M2M Platform, obliterates the need of a management layer to be created on top of all the applications besides adding values like interoperability, security, data management etc.

The issue with IoT interoperability is diversity



Source: AIOTI WG3 (IoT Standardisation) – Release 2.7

Horizontal Cross Domain Interoperability



- Highly fragmented market with small vendor-specific applications.
- Reinventing the wheel: Same services developed again and again.
- Each silo with its own technologies without interoperability.

- End-to-end platform: common service capabilities layer.
- Interoperability at the level of communications and data.
- Seamless interaction between heterogeneous applications and devices.

What is oneM2M ?

- A global partnership among Standards Defining Organizations (SDOs) and Industry Associations like :

  ARIB (Association of Radio Industries and Businesses, Japan),
  ATIS (Advancing Transformation of the ICT Industry, America),
  CCSA (China Communications Standards Association, China),
  ETSI (European Telecommunications Standards Institute, Europe),
  TIA (Telecommunication Industries Association, America),
  TSDSI (Telecommunications Standards Development Society, India),
  TTA (Telecommunications Technology Association, Korea), and
  TTC (Telecommunications Technology Committee, Japan).

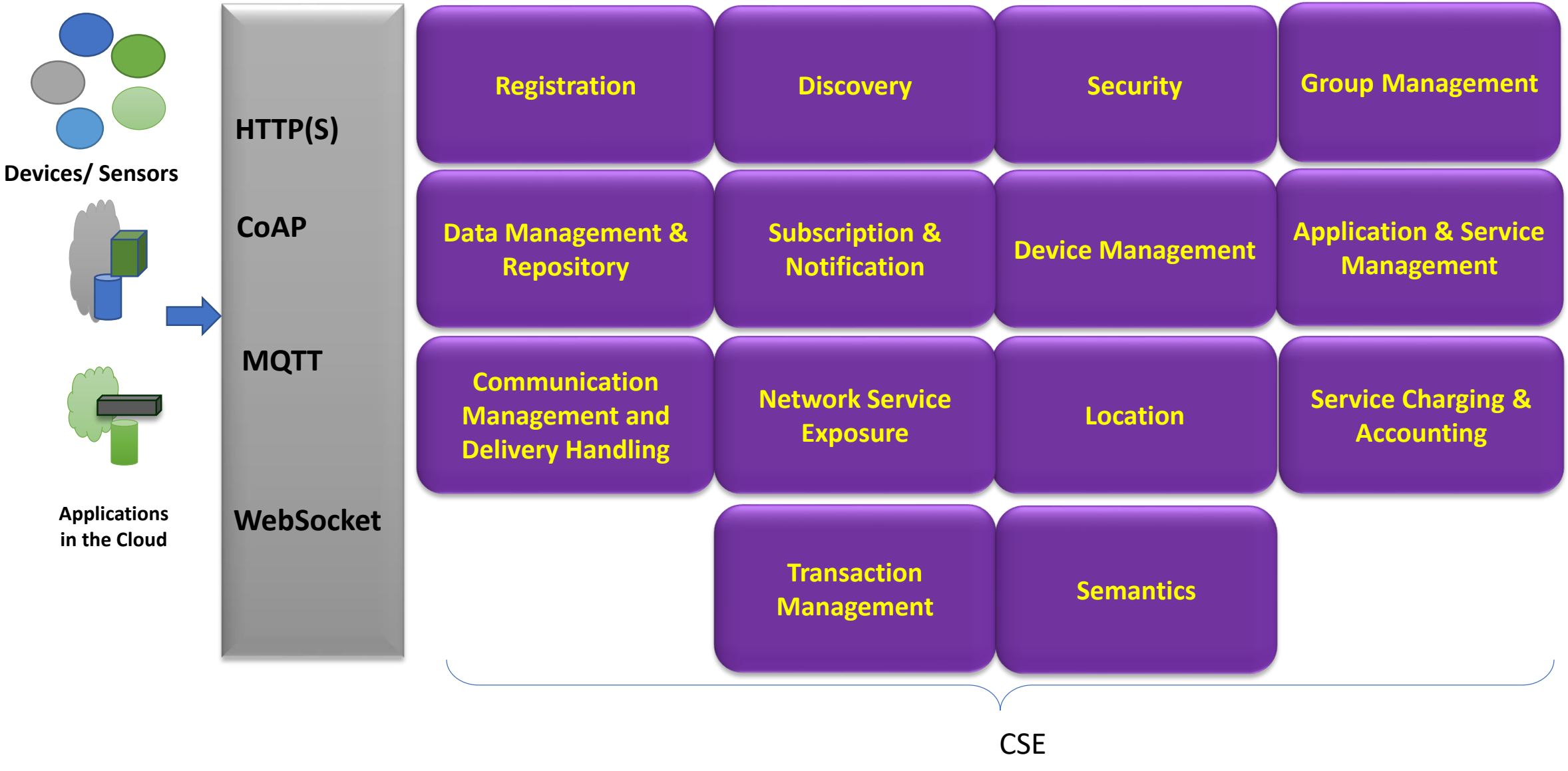
  Additional partners contributing to the oneM2M work include:

  the BBF (Broadband Forum), Continua, GlobalPlatform, HGI (Home Gateway Initiative), the New Generation M2M Consortium - Japan, and OMA (Open Mobile Alliance).

  [C-DOT is also partner Type I (through TSDSI) contributing to the standards]

- **In simple terms the main goal to develop technical specifications for an M2M Service Layer**
  - A software platform to make M2M devices/applications communicate with each other in a secure and efficient manner

The Common Service Functions in oneM2M Architecture



Strong Implementation Base

Industry-driven Open source implementations

LAAS-CNRS

Fraunhofer FOKUS

KETI

CISCO

OM2M Connecting things

open mtc

OCEAN

OPEN DAYLIGHT IotDM

Examples of Commercial implementations /demos

LG

सी-डॉट C-DOT

सेंटर फॉर डेवलपमेंट ऑफ टेलीमैटिक्स
Centre for Development of Telematics

PILOT THINGS

SIERRA WIRELESS

InterDigital

QUALCOMM

kt

HUAWEI

SK telecom

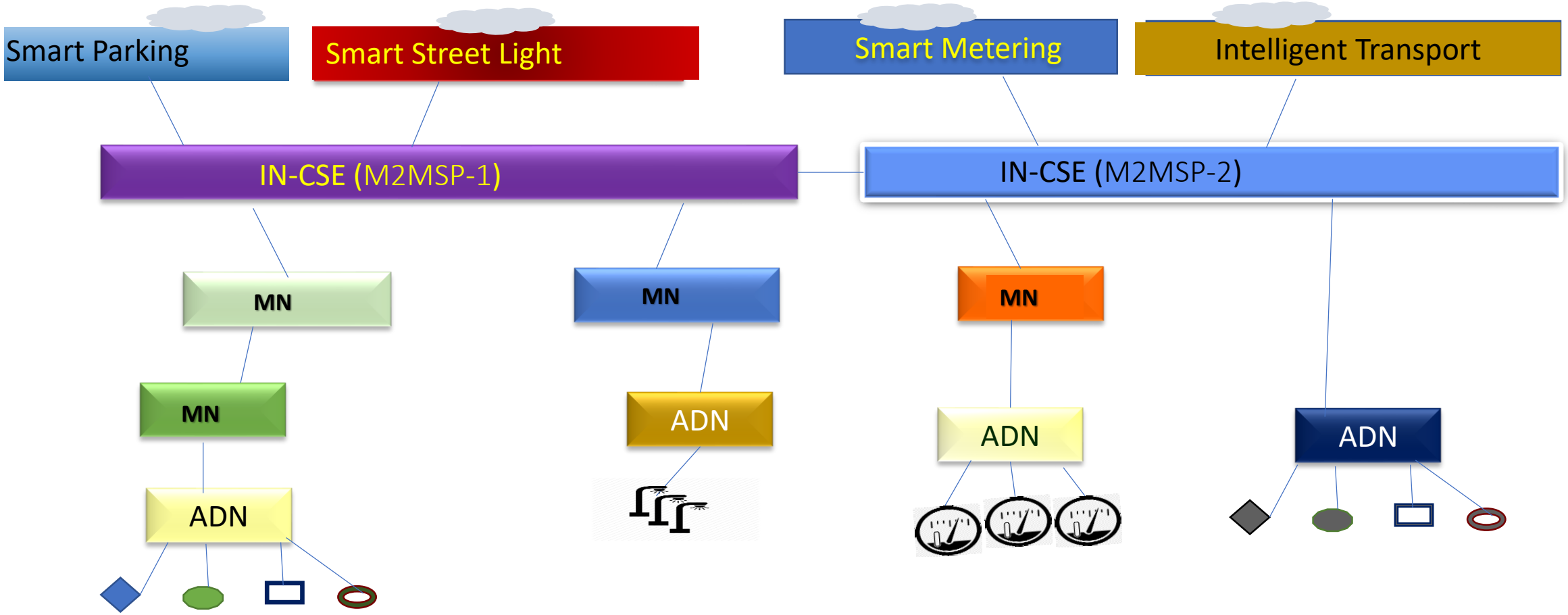
sensinov Global IoT Platform

MODACOM

LG U+

Hewlett Packard Enterprise

Deployment of IoT Applications : the oneM2M way



MN-Middle Node :oneM2M Gateway Device (Contains CSE and optionally applications)

ADN-Application Dedicated Node :The oneM2M Device that contains applications which interface with sensors/actuators

oneM2M Feature Summary by Release

Rel-1 Features

- Registration
- Discovery
- Security
- Group Mgmt.
- Data Mgmt. & Repository
- Subscription & Notification
- Device Management
- Communication Mgmt.
- Service Charging
- Network Service Exposure
- App & Service Mgmt.
- HTTP/CoAP/MQTT Bindings

Rel-2 Features

- Time Series Data
- Flexible resources that can be customized by app developers
- Semantics Description & Discovery
- Security Enhancements
  - Dynamic Authorization
  - Content Security
  - E2E Security
- WebSocket Binding
- Ontology for Home Area Information Model
- oneM2M App-ID Registry
- oneM2M Interworking
  - LWM2M
  - AllJoyn
  - 3GPP Triggering

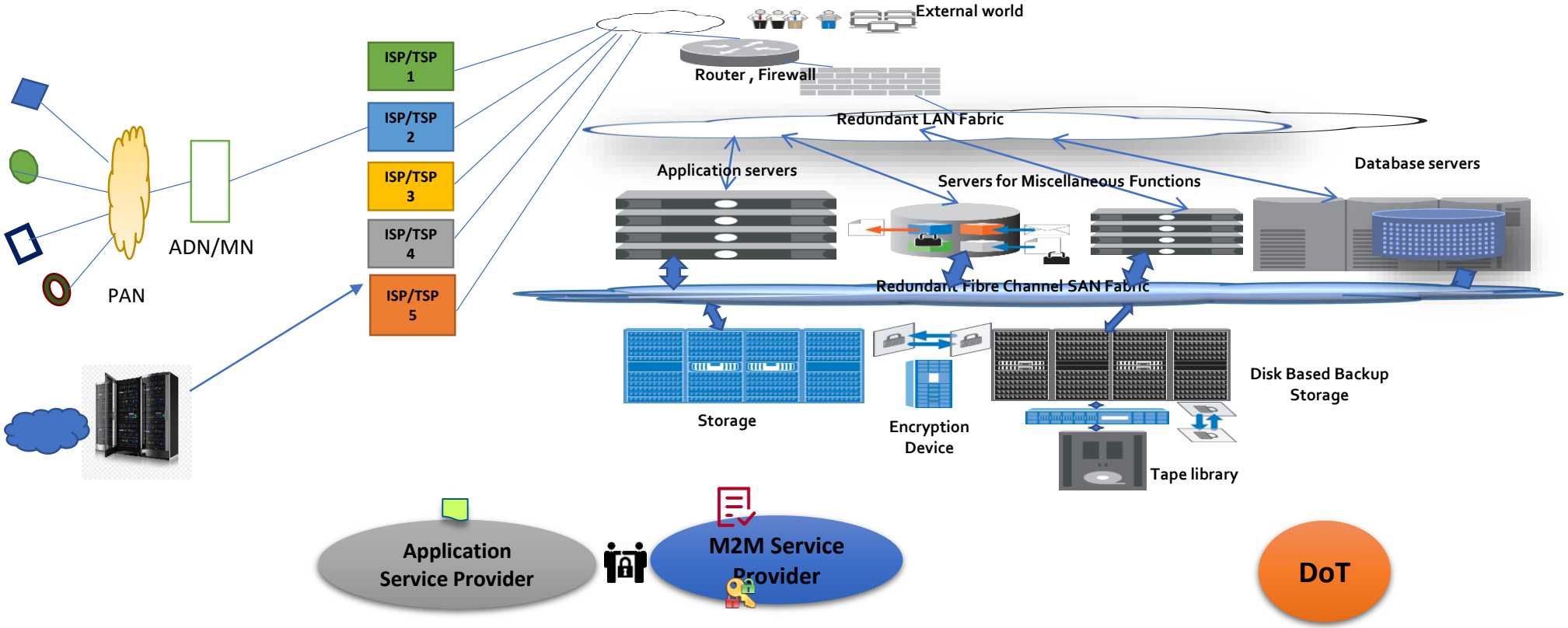
Rel-3 Features

- Semantic Querying/Mashups
- 3GPP SCEF Interworking
  - Non-IP Data Delivery,
  - UE Reachability Monitoring
  - Device Triggering
  - Etc.
- Transaction Management
- Service Layer Routing
- Common oneM2M Interworking Framework
  - OCF, OPC UA, OSGi, Modbus
- oneM2M Conformance Tests and Profiles
- Security Enhancements
  - Distributed Authorization, etc.
- Ontology-based Interworking

Rel-4 Features (planned)

- Fog/Edge Computing
  - Service Provisioning
  - Service Pooling, etc.
- 3GPP Interworking
  - Session QoS
  - V2X
  - NIDD Enhancements
  - Charging
- Vehicular Centric Features
  - Mobility, low latency, …
- Semantic Reasoning & Ontology Mapping
- Service/User Subscription
- Security Enhancements
  - User/Data Privacy, etc.
- W3C WoT Interworking
- SDT4.0 and the information models for multiple domains
- Streamlining oneM2M protocol
- oneM2M Conformance Tests

Deployment of Standardised M2M/IoT Ecosystem



1. M2M Service Provider registers with DoT fulfilling the M2MSP registration Process(Licensed or otherwise!!)
2. Sets up M2M Platform Infrastructure with the common service functions
3. Ties up with one or many TSPs/ISPs for connectivity
4. Application Service Provider(s) approaches M2MSP with their intended application and signs an agreement. The agreement binds them for application enrolment and registration, Access Control Policies, use of security framework, device management, discovery and other CSFs besides commercial agreements.
5. The ASPs get the Unique AE-ID, Encryption Keys for their application entities
6. The ASPs set up their IN-AE on their platform of choice(Public or private infrastructure).
7. The ASPs roll out devices & applications in the field

Benefits of using oneM2M Standard

The following are achieved when we use oneM2M based architecture

- Interoperability of devices and applications
- Only authenticated and authorized devices can communicate
- Information and statistics regarding devices and applications would be available
- Resource utilization can be monitored
- Regulations, KYC can be enforced
- Certification would become feasible (with standardized test suites) for
  - *Devices: Ecosystem of Certified products ensuring interoperability, trust*
  - *Applications: Sharing of data, interworking, Security*
  - *Services: Compliance*
- Data Security and Privacy concerns are addressed in the architecture itself (Lawful interception would also become possible)
- Data sharing among divergent applications
- Integration of divergent applications
- Device Management becomes easy

What happens if oneM2M is not Adopted

Interoperability: Device, Network and Application Level Interoperability can not be achieved. Universal pluggability can not be achieved

Security: We would not be able to prevent deployment of unauthorized and unauthenticated devices and applications in the network which may be a serious threat to the entire ecosystem(and to the mankind)
Due to non-standardized implementation, security (including lawful interception) can not be ensured

Benefits to Local Entrepreneurs: Startup community would not be able to bring innovations as proprietary interfaces make application development time-consuming, difficult and expensive

Regulations: Implementation of KYC norms would be extremely difficult. No control over unregulated proliferation of devices and applications

Monetization: Monetization of the M2M Service Provider, Application Service Provider, Device Manufacturers would not be structured and clear

Licensing: Low-touch-licensing would become no-touch-licensing

Transparency: Obtaining details and statistics about the devices, applications and services would be extremely difficult .

THANK YOU

AURINDAM BHATTACHARYA
GL, C-DOT

aurindam@cdot.in