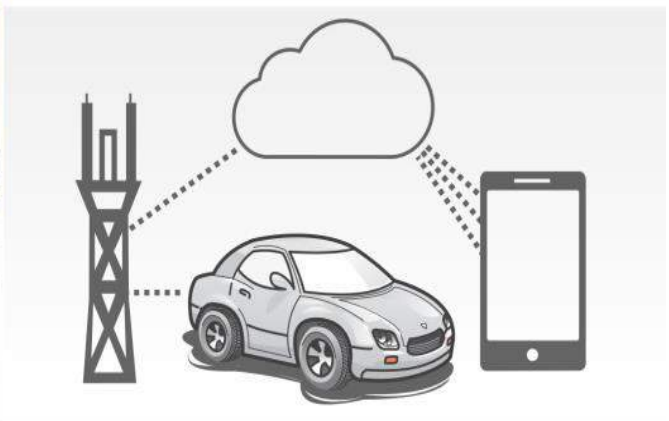
सत्यमेव जयते

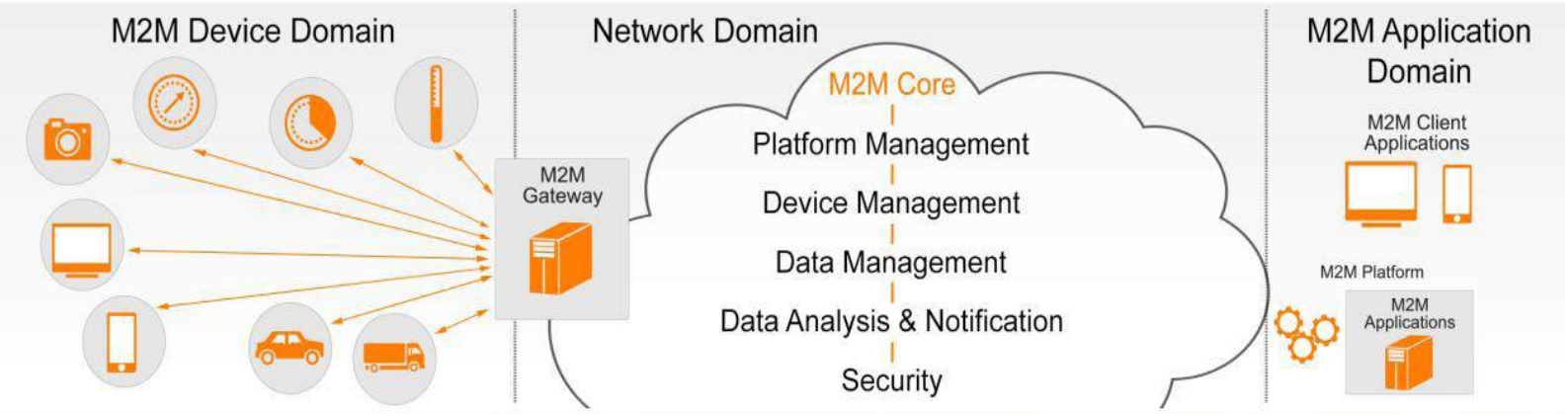
TECHNICAL REPORT

M2M GATEWAY & ARCHITECTURE

TEC-TR-S&D-M2M-001-01

M2M GATEWAY & ARCHITECTURE WORKING GROUP





ISO 9001:2008

TELECOMMUNICATION ENGINEERING CENTRE
DEPARTMENT OF TELECOMMUNICATIONS
MINISTRY OF COMMUNICATIONS & INFORMATION TECHNOLOGY
GOVERNMENT OF INDIA

RELEASE 1.0

MAY 2015

Revision History

Date	Release	Document No.	Description
12-05-2015	R1.0	TEC-TR-S&D-M2M-001-01	Technical report on M2M Gateway & Architecture.

Important Notice

Individual copies of the present document can be downloaded from **http://www.tec.gov.in**
Users of the present document should be aware that the document may be subject to revision or change of status.
Any comments/suggestions may please be sent to:**m2mreports.tec@gov.in**

Disclaimer

The information contained is mostly compiled from different sources and no claim is being made for being original. Every care has been taken to provide the correct and up to date information along with references thereof. However, neither TEC nor the authors shall be liable for any loss or damage whatsoever, including incidental or consequential loss or damage, arising out of, or in connection with any use of or reliance on the information in this document. In case of any doubt or query, readers are requested to refer to the detailed relevant documents.

रवि शंकर प्रसाद
RAVI SHANKAR PRASAD

सत्यमेव जयते

मंत्री
संचार एवं सूचना प्रौद्योगिकी
भारत सरकार
MINISTER
COMMUNICATIONS & IT
GOVERNMENT OF INDIA

Message

I am glad to note that Telecommunication Engineering Centre is bringing out Technical Reports on M2M enablement in Transport, Health, Power and Safety & Surveillance sectors and a Report on M2M Gateway & Architecture.

M2M communications is going to change the way the humans live and control their surrounding as well as various social and economic sectors operate. It is expected to improve the efficiency of various sectors such as Automotive, Health, Power and Safety & Surveillance etc. by transmitting the information electronically and automation of information processing. It will help in providing quality sevices to our citizens.

I am confident that the Technical Reports will help in developing specifications/ standards to be used in India and opportunity of manufacturing wide variety of devices and other products in India. I congratulate TEC and all concerned for this commendable work which is very timely, and wish them success in all their endeavors.

(RAVI SHANKAR PRASAD)

Room No.: 105, Sanchar Bhawan, 20, Ashoka Road, New Delhi - 110001
Phone : 91-11-23739191, 23372177 Fax : 91-11-23723330

राकेश गर्ग
सचिव
RAKESH GARG
Secretary

सत्यमेव जयते

भारत सरकार
Government of India
संचार एवं सूचना प्रौद्योगिकी मंत्रालय
Ministry of Communications &
Information Technology
दूर संचार विभाग
Department of Telecommunications

08th May 2015

Message

I am extremely happy to note that Telecommunication Engineering Centre (TEC) is bringing out Technical Reports regarding M2M enablement in Intelligent Transport System, Health, Power, Security and Surveillance and a Technical Report on Gateway an Architecture of M2M communications.

2. While Government started the work of developing roadmap for M2M communications in India, TEC at the same time initiated the work of identifying technical requirements of Automotive, Health, Power, Safety and Surveillance sectors. As there has been active participation from stakeholder of each sector, the reports have taken into account the ground level status and requirement for M2M enablement.

3. India has to make strides in making its various sectors smart for which quick adoption of M2M is the necessary. These reports will help stakeholders in development and finalization of sectors specific plans for adoption of M2M.

4. I appreciate the efforts put in by Telecommunication Engineering Centre in bringing out these reports. I wish them success in all their endeavours.

(Rakesh Garg)
Secretary(Telecom)

संचार भवन, 20, अशोक रोड़, नई दिल्ली-110001 / Sanchar Bhawan, 20, Ashoka Road, New Delhi-110001
Tel. : 011-23719898, Fax : 011-23711514, E-mail : secy-dot@nic.in

सत्यमेव जयते

सदस्य (प्रौद्योगिकी) एवं
पदेन सचिव, भारत सरकार
Member (Technology), Telecom Commission &
Ex-Officio Secretary to Govt. of India
Tel : 23372307 Fax : 23372353

भारत सरकार
संचार एवं सूचना प्रौद्योगिकी मंत्रालय
दूरसंचार विभाग
संचार भवन, २०, अशोक रोड़,
नई दिल्ली.११०००१
Government of India
Ministry of Communications & Information Technology
Department of Telecommunications
Sanchar Bhawan, 20, Ashoka Road,
New Delhi-110001

Message

I am happy to note that Telecommunication Engineering Centre (TEC) is bringing out technical reports regarding M2M enablement in Intelligent Transport System, Health, Power, Security and Surveillance and a report of Gateway an Architecture of M2M communications. We are aware that adoption of M2M communication will inter-alia, lead to enhancement in the efficiency of various sectors of society and economy.

Need for improvement in efficiency in various socio-economic sectors has been felt for a long time and some efforts in this direction have also been made whereby M2M based systems have been deployed. However, the solutions which have been implemented are generally based on propriety platforms. However, to achieve smart processes and functioning in all the sectors, interoperability of devices/ platforms/ applications is necessary which entails adoption of open standards.

The technical reports of TEC are a good step in this direction and will certainly help various stakeholders to take preparatory steps in their respective sectors for future adoption of M2M communications.

S. S. Sirohi

(S.S. Sirohi)
Member (T)
8.5.2015.

सलाहकार (प्रौद्योगिकी)
Advisor (Technology)
Tel. : + 91-11-23718460
+ 91-11-23036317
Fax : + 91-11-23329525

सत्यमेव जयते

भारत सरकार
संचार एवं सूचना प्रौद्योगिकी मंत्रालय
दूरसंचार विभाग
संचार भवन, नई दिल्ली-110 001
Government of India
Ministry of Communications &
Information Technology
Department of Telecommunications
Sanchar Bhawan, New Delhi-110 001

A.K. Bhargava
Advisor, DoT

Message

I am pleased to note that Telecommunication Engineering Centre (TEC) is bringing out Technical Reports regarding M2M enablement in Intelligent Transport System, Health, Power, Security and Surveillance and a report on Gateway & Architecture of M2M communications.

TEC has taken timely action to take up the work of study and preparation of the Technical Reports in the Automotive, Health, Power, Safety and Surveillance sectors. The Reports have been prepared to be released along with the National M2M roadmap by virtue of relentless efforts of TEC and its Working Groups consisting of stake holders.

M2M communication is an opportunity for India not only to keep pace with the world but also to march ahead in development of specifications of new products consisting of Devices, Gateways and Platforms meeting the Indian requirements, though of course, in sync with the standards.

I appreciate the efforts of Telecommunication Engineering Centre specially its S&D Division and all the Working Groups for bringing out these technical reports in a very timely manner. I wish them success in all their endeavours.

(A.K. Bhargava)

AJAY KUMAR MITTAL
वरिष्ठ उप महानिदेशक
Sr. Deputy Director General
Tele : 23320252 Fax : 23329088
e-mail : srddg.tec@gov.in
www.tec.gov.in

सत्यमेव जयते

भारत सरकार
दूरसंचार विभाग
दूरसंचार इंजीनियरी केन्द्र
खुर्शीद लाल भवन, जनपथ, नई दिल्ली–110001
Government of India
Department of Telecommunications
Telecom Engineering Centre
Khurshid Lal Bhawan, Janpath, New Delhi-110001
ISO 9001:2008

FOREWORD

Telecommunication Engineering Centre (TEC) is an organ of Department of Telecommunications (DoT). It provides technical support to DoT. TEC develops technical specifications of products for use in telecom networks. It carries out technology studies and proactively takes up development of specifications based on such studies Development of specifications is a transparent process with active participation of stakeholders. Certification of telecom products is also one of its activities.

M2M Communication is an area which has rapidly attracted attention of world over, primarily due to its enormous potential in bringing about fundamental changes in the delivery and use of services in almost all sectors of economy and society and the quality of human life.

M2M systems have been in use for some time past, e.g. in automotive sector. However, the use of technology/devices/application is generally proprietary in nature as standards have started involving in the recent past. We are aware that variety of social and economic activities are interdependent and in today's digital world, it is possible to link them through networks and applications to achieve enhancement in efficiency and development of new services. This is possible only when there is interoperability among devices/networks/applications. This requires standardization and development of harmonized specifications.

Towards achieving this objective, TEC in consultation with stake holders from government, industry, standards bodies and sector users, took up study of four sectors to begin with namely Automotive, Health, Power, Safety and surveillance. Four working groups (WG), one for each were formed with the participation from stakeholders as mentioned above. As it is also necessary to work out architecture for M2M domain and also service delivery models, Gateway and Architecture WG was also formed. All the groups have overwhelming participation. Chairmen, Rapporteurs & Co-rapporteurs have been elected by the WGs themselves. Joint Working Group is chaired by Sr. Deputy Director General and Head TEC.

These groups have carried out use case studies and analysis for respective sectors. Beginning the year 2014, these groups have worked relentlessly. This can be gauged from the fact that there were about 50 conference calls and four Face to Face (F2F) meetings combined of all groups and lot of many interactions within the groups. Services and Development (S&D) Division of TEC coordinated and managed the entire activity of formation of working groups, holding meetings, preparation of the reports etc.

The reports contain use cases in the sectors & their technical analysis, key challenges in implementation and the way forward. Suggestions for way forward those have emerged, require action by various stake holders as well as by TEC and the Working Groups. TEC and the Working Groups will continue further work and it is planned to bring out next release of Technical Report after further study as early as possible.

I express my sincere thanks to all the Chairmen, Rapporteurs and Co-rapporteurs and members of the Working Groups as well as the participating stakeholders as organization and as persons whose enthusiastic support and untiring efforts have made it possible to bring out these detailed reports.

Ultimate aim is to identify the areas for development of standards, harmonize Indian standards with international standards and development of product specifications ensuring interoperability. India being a big market for M2M, there is enormous potential of manufacturing devices and networking products for M2M in India. Let us all join hands to become part of the 'Make in India' programme of the Government of India.

I hope that the report will provide guidance to the stakeholders to plan standardized deployments in the concerned sectors. I also hope that the stake holders will provide their continued support to TEC to carry out further work in M2M domain. We will be enriched in our work through valuable suggestions from any quarter.

(A.K.Mittal)
Sr. Deputy Director General & Head
Telecom Engineering Centre

Contents

Figures

Tables

List of Contributors

A. Joint Working Group (JWG) Chairman:

Name	Designation	Organisation	E-mail Address
Ajay Kumar Mittal	Sr.DDG	Telecommunications Engineering Centre (TEC)	srddg.tec@gov.in

B. Joint Working Group (JWG) Secretariat:

Name	Designation	Organisation	E-mail Address
Sushil Kumar	DDG(S&D)	Telecommunications Engineering Centre (TEC)	ddgsd.tec@gov.in

C. Working Group (WG) Chairs:

	Name	Organisation	E-mail Address
Chairman	Sriganesh Rao	Tata Consultancy Services Limited(TCS)	sriganesh.rao@tcs.com
Rapporteur	Aurindam Bhattacharya	Centre for Development of Telematics(C-DOT)	aurindam@cdot.in
Co-Rapporteur	P. S. Jadon	Telecommunications Engineering Centre (TEC)	dirr2.tec@gov.in

D. Primary Authors

Name	Organisation	E-mail Address
Anupama Chopra	C-DOT	anupama@cdot.in
Aurindam Bhattacharya	C-DOT	aurindam@cdot.in
Niranth Amogh	Huawei	namogh@huawei.com
Sriganesh Rao	TCS	sriganesh.rao@tcs.com

E. Contributors

S.No.	Name	Organisation
1	Ajay Kumar Mittal	TEC
2	Alok Mittal	STMicroelectronics
3	Anirban Ganguly	TTSL
4	Anuj Ashokan	TTSL
5	Ashwani Kumar	Ericsson
6	Hem Thukral	ISGF
7	P. S. Jadon	TEC
8	Narang N. Kishore	Narnix Technolabs
9	Mukesh Dhingra	TTSL
10	Neelesh Manthri	TTSL
11	Rajeev Kumar Tyagi	TEC
12	Sushil Kumar	TEC

F. Joint Editorial Team:

S.No.	Name	Organization
1	Ajay Kumar Mittal	TEC
2	Sushil Kumar	TEC
3	Aurindam Bhattacharya	C-DOT
4	Anuj Ashokan	TTSL
5	Sriganesh Rao	TCS
6	Niranth Amogh	Huawei
7	Hem Thukral	ISGF
8	Alok Mittal	STMicroelectronics
9	Rohit Singh	Smart 24*7
10	Sharad Arora	TTSL
11	Rajeev Kumar Tyagi	TEC

Executive Summary

Machine to machine (M2M) communication is considered to be a huge market with immense potential for growth and a key enabler of applications, innovations and services across a broad range of sectors. The need was to create a standard for M2M communication which would make interoperability a reality and would provide a much needed boost to the manufacturing and services sector in India. Standardisation activity is picking up and across the world. India being a large potential user of M2M communications, needs to ensure that the standards take into account India specific requirements. Telecom Engineering Centre (TEC) proffered for framing specifications for M2M in India. Five Working Groups (WGs) were formed namely Automotive, Power, Health, Surveillance and Gateway & Architecture (G&A). M2M Gateway & Architecture WG is supposed to play its role in all sectors and would work as a horizontal layer. The Scope of the G&A WG included identification of a minimum set of common requirements of vertical markets and defining a common M2M service layer to provide a cost-efficient platform, which can be easily deployed in hardware and software, in a multi-vendor environment, and across sectors.

The following activities were performed by Gateway & Architecture WG:

- Exhaustive and in-depth discussions were held over conference calls and face to face meetings on various architecture options available for M2M communication.
- The popular and widely accepted OneM2M architecture was studied to see if that fits all the use case scenarios of various verticals.
- A Use Case capturing template was created and circulated to all sectoral WGs. The current use cases were studied and then mapped in the architecture. Discussions were held towards naming and addressing. Use of separate category of SIMs for M2M was also deliberated. The issues in regulatory framework, spectrum usage and need for additional frequency spectrum were also discussed. The use of IPv6 in the M2M architecture was deliberated

This Report:

- Provides analysis for OneM2M architecture with respect to a more generic M2M architecture and its various deployment scenarios.
- Identifies the means to realize a common service layer architecture for different sectors
- Provides reference for different sectors to understand the architectural implications of OneM2M for designing the common service layer.

In the end the way forward has been suggested for adopting OneM2M architecture as base and for further deliberations on the issues of naming and addressing, security, network and spectrum.

1. Introduction

The M2M market is segmented and most of the M2M solutions have been designed for vertical/industry specific applications. This affects the development of large scale M2M solutions. The M2M device space is growing tremendously, thus introducing a wide variety of disparate M2M devices in the market. It poses many technical challenges in terms of security, device data management, discovery, etc. There is tremendous growth opportunity for M2M applications and also for low cost M2M devices having reasonable computing power coupled with long lasting battery.

2. Scope and Purpose

This document analyses various network architecture models being deployed for M2M applications in various industry segments in almost all possible deployment scenarios. It also attempts to identify the gaps between these architectures with respect to the Common Service Layer Architecture proposed by OneM2M. The common M2M Service layer is standardized by oneM2M, a global organization created to develop a scalable and interoperable standard for communications of devices and services used in M2M applications and the IoT. It was formed in 2012 by seven of the world's preeminent standards development organizations. To develop a common architecture, the following oneM2M Partner standards development organizations have contributed to Architecture Analysis [5] and Architecture Merging [6]:

- ARIB (Japan)
- ATIS (U.S.)
- CCSA (China)
- ETSI (Europe)
- TIA (U.S.),
- TTA (Korea)
- TTC (Japan)
- TSDSI (India) - new oneM2M Partner Type 1

Additional partners contributing to the oneM2M work include:

- BBF (Broadband Forum)
- Continua
- HGI (Home Gateway Initiative)
- New Generation M2M Consortium - Japan

OMA (Open Mobile Alliance)

This document will serve as reference for different verticals/industries to understand the architectural implications of oneM2M for designing the common service layer.

This document will also serve as reference for TEC to derive the "Generic Requirements" for oneM2M compliant M2M Gateway and Platform systems.

3. Terms and Abbreviations

3GPP	3rd Generation Partnership Project
6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
AE	Application Entity
AHD	Application Hosting Device
ANT	Proprietary wireless technology Protocol
API	Application Programming Interface
ASP	Application Service Provider
ASN	Autonomous system number
AS Node	Application Server Node
AUE Node	Application User Equipment Node
AVAG	Audio Video Alarm Gateway
BT	Bluetooth
BTLE	Bluetooth Low Energy
CoAP	Constrained Application Protocol
CSE	Common Services Entity
CSF	Common Services Function
DCU	Data Concentrator Unit
DG	Device Gateway
DOT	Department of Telecom
DSL	Digital Subscriber Line
DVR	Digital Video Recorder
E2ESP	End to End M2M Service Provider
ECG	ECG Electrocardiography
EHR	Electronic Health Record
EMR	Electronic medical records
GPRS	General Packet Radio Service
GSM	Global System for Mobiles
FP	Field Provider
HATEOAS	Hypermedia as the Engine of Application State
HCD	High Capability Node
HIE	Health information exchange
HTTP	Hyper Text Transfer Protocol
HRN	Health Record Network
IDG	Interaction between Device and Gateway
IETF	Internet Engineering Task Force
IGG	Interaction between two Gateways
IGP	Interaction between Gateway and Platform
IMN	Interaction between M2M layer and underlying Network
IP	Internet Protocol

IPA	Interaction between Platform and Application
IP-CAN	Internet Protocol Connectivity Access Network
IPE	Internetworking Proxy Entity
IPP	Interaction between two Platforms
ITU	International Telecommunications Union
ISM	Industrial, Scientific and Medical Band of Spectrum (like 2.4GHz, 865-868MHz)
IVR	Interactive Voice Response
LAN	Local Area Network
LCD	Low Capability Device
M2M	Machine-to-Machine
MN	Mobile Node
MSO	Multi Service Operator
M2M SP	M2M Service Provider
MQTT	Message Queue Telemetry Protocol
NAN	Neighborhood Area Network
NFC	Near Field Communication
NOC	Network Operation Centre
No LCD	Non-oneM2M Low Capability Device
NSE	Network Service Entity
NSP	Network Service Provider
N&SP	Network and Service Provider
PAN	Personal Area Network
PG	Platform Gateway
PHI	Protected Health Information
PLC	Power Line Carrier
PSP	Platform Service Provider
QoS	Quality of Service
QOL	Quality of Life
REST	Representational State Transfer
RFID	Radio Frequency Identifier
RMD	Remote Monitoring Device
SAG	Sensor & Alarm Gateway
SMS	Short Message Service
Sub-Gig	Sub Giga Hz Radio Communication
TAN	Touch Area Network
TCP / IP	Transmission Control Protocol/ Internet Protocol
TEC	Telecom Engineering Centre
UDP	User Datagram Protocol
USB	Universal Serial Bus
WAN	Wide Area Network

4. M2M Architecture

4.1 Concept

The M2M ecosystem is considered to be organized in a 3-Layer conceptual model as shown in the Figure 1 below. It consists of:

- Network Services Layer: Provided by the Network Service Provider.
- M2M Services Layer: Based on Internet Protocol (IP) and provided by the M2M Service Provider. (*The development of this layer is the key focus area towards standardization of M2M communications*) Application Layer: Provided by the Application Service Provider catering to End User Applications.

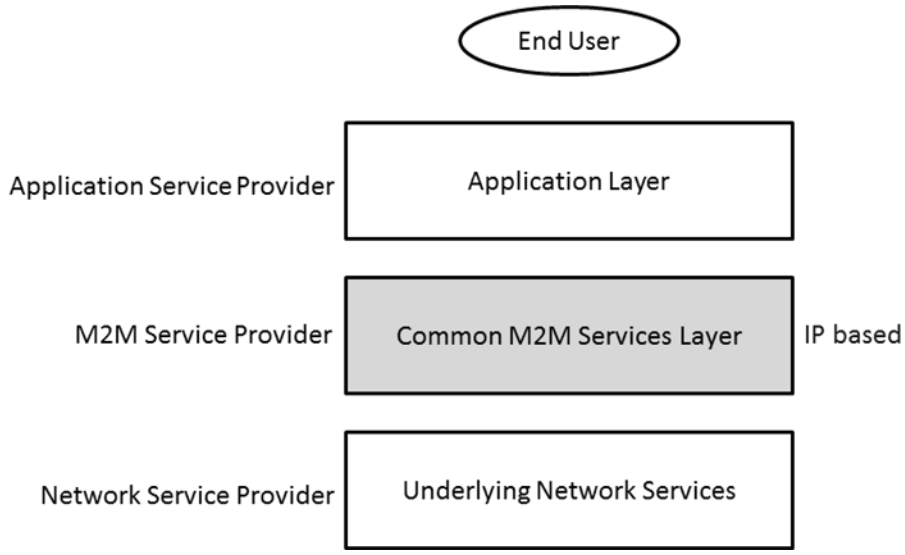


Figure 1: M2M Conceptual Model

4.2 Generic M2M Network Architecture Model

In line with the conceptual model indicated above, a typical M2M network architecture model is as shown in the Figure 2 which currently prevails in the M2M markets:

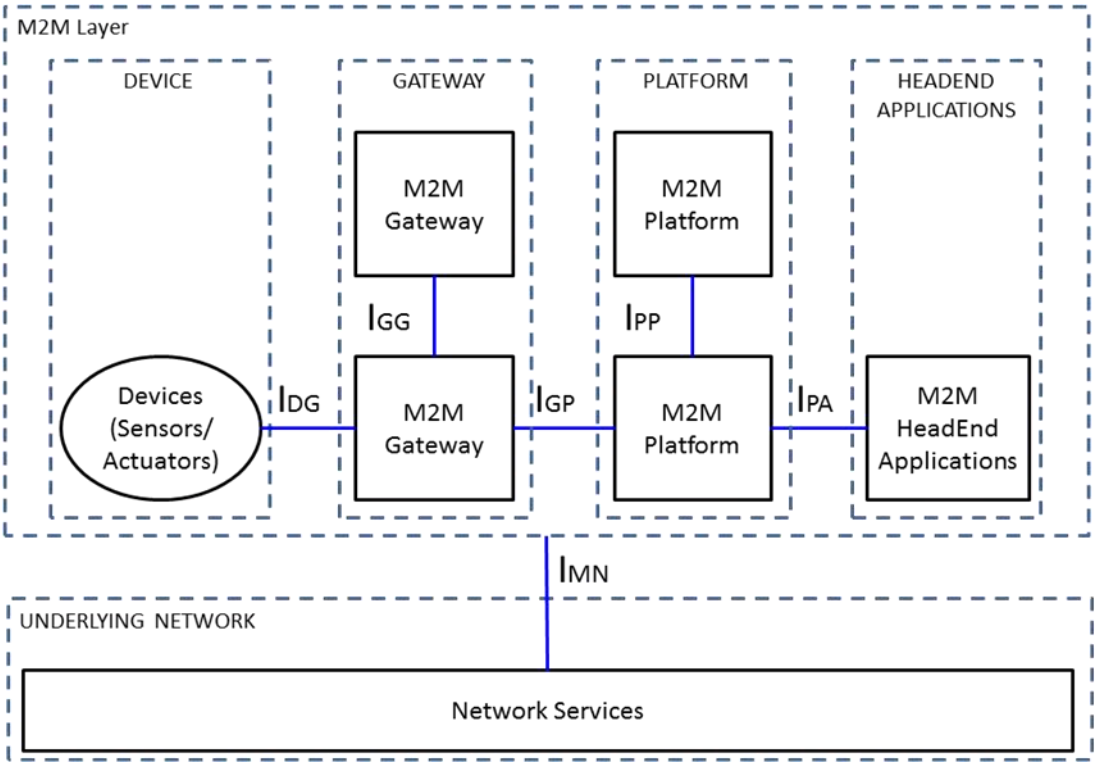


Figure 2: General M2M Network Architecture

The key components of the model and their respective functionalities are as described below:

- **Device**: It represents all the device entities like the sensors, actuators, etc. These entities are responsible for generating information (content, data) pertaining to the environment which is the field of observation or some actuations without human intervention. They generally communicate with a Gateway entity to send the sensed/informed or receive commands to perform some actions.
- **Gateway**: It represents the entities which are responsible to aggregate the device information and provide them to the Platform. It is also responsible to communicate the commands received from the Platform to the devices.
- **Platform**: It represents some common set of services which perform control, application support and management functions in a M2M service environment. e.g., Device management, Service management, Location management, Discovery, Application Routing, Security, Charging, Service Exposure APIs, etc. The platform shall support services which cater to different vertical applications (Home, Health, Industrial Automation, Transport, Power, etc.)
- **Head-end Applications**: It represents the end user applications for the concerned use cases of respective verticals (Home, Health, Industrial Automation, Transport, Power, etc.).

- **Underlying Network**: It represents entities which provide network related services. (E.g. PAN, IP-CAN, Charging, Device triggering, location, etc.)

Physical interfaces in the General M2M Network Architecture framework can be represented as:

- IDG: It facilitates interactions between the Device and the Gateway. From the underlying network perspective it may use diverse connectivity services like PAN, IP-CAN, etc.
- IGP: It facilitates interactions between the Gateway and the Platform. This is IP based communication.
- IGG: It facilitates interactions between two Gateways. This is IP based communication.
- IPA: It facilitates interactions between the Platform and the Application. This is IP based communication.
- IPP: It facilitates interactions between two Platforms. An IPP (SP) may be used to facilitate interactions between different M2M service providers. This is IP based communication.
- IMN: It facilitates interactions between the M2M layer and the Underlying network. The Device and Gateway domain entities may have more than one type of underlying network connectivity which can be used for communication with the Platform. The underlying networks may provide common services like location, charging, device triggering, etc to the M2M layer and will utilize the respective interfaces defined in 3GPP, IETF, etc.

4.3 Analysis of M2M Network Architectures for Verticals/Industry

4.3.1 Power

The M2M network architecture for Advanced Metering Infrastructure (AMI) is illustrated in Figure 3.

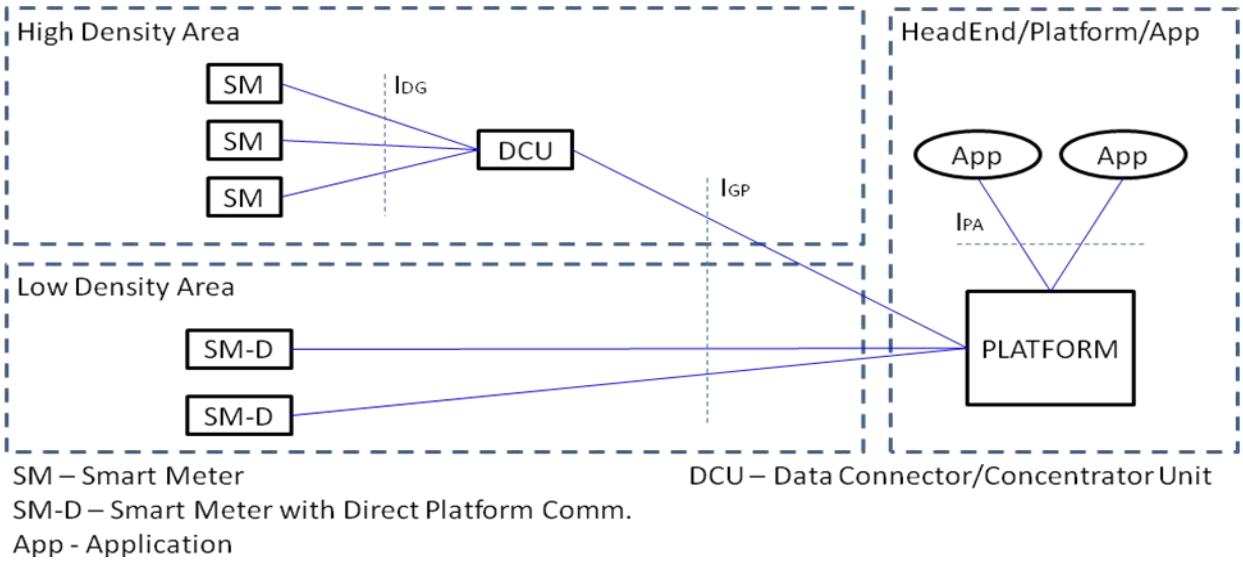


Figure 3: Power Vertical M2M Network Architecture

The Field side of the M2M network for AMI can be classified as High Density Area for metropolitan areas, cities and apartments; Low Density Area for rural areas, Industries and Enterprises which not only includes power deployed for Brick and Mortar industry but also the Substations.

The Field area (Smart Meter to DCU) connectivity varies for different area deployments. Example:

Area	Connectivity
High Density Area	Fixed (PLC, RS 485etc) Wireless (ZigBee, Wi-Fi, 6LoWPAN etc.)
Low Density Area	Wireless (ZigBee, Sub-GHz, GPRS etc) Fixed (PLC etc.)

Table 1: Power Sector Field Area Connectivity

The Operator area (DCU to Platform) connectivity has the following options.

Area	Connectivity
High Density Area	Fixed (Ethernet over Optical, Ethernet, DSL) Wireless (3G, GPRS etc)
Low Density Area	Wireless (3G, GPRS etc)

Table 2: Power Sector Operator Area Connectivity

4.3.2 Health

The M2M network architecture model for health vertical is illustrated in Figure 4.

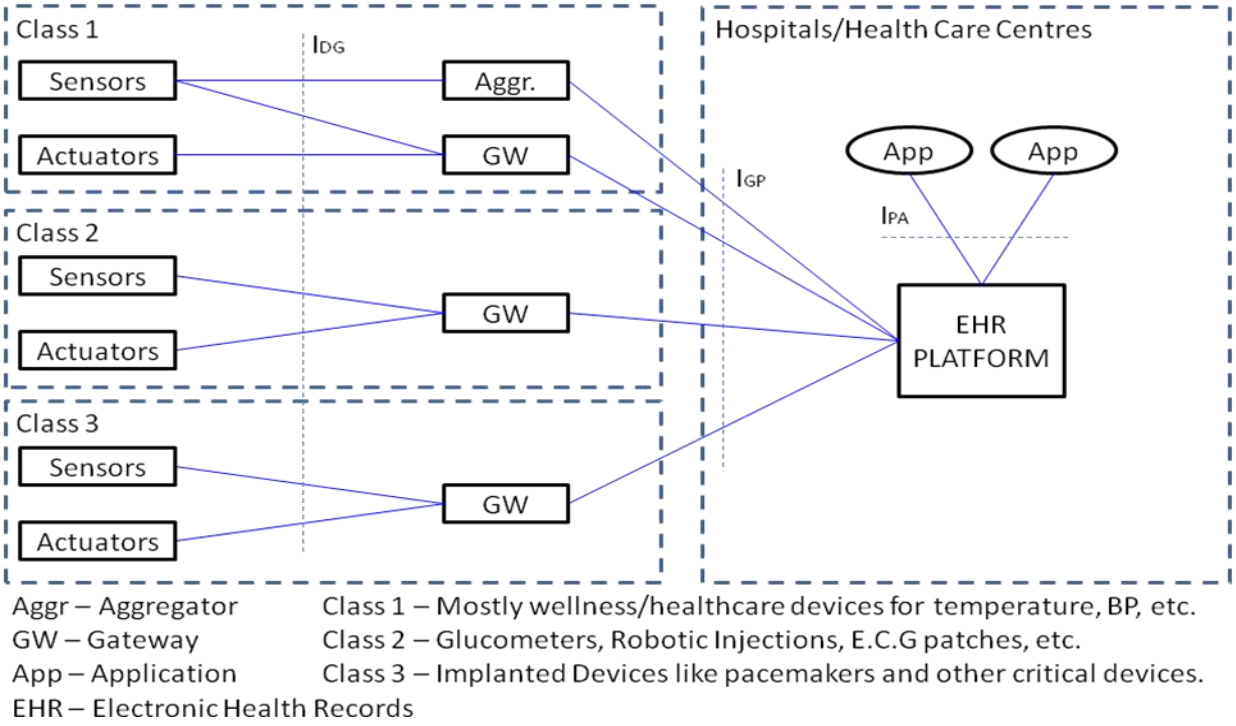


Figure 4: Health Vertical M2M Network Architecture

The Field side of the M2M network for health can be classified as Class 1, Class 2 and Class 3 [8]. The devices of these classes are connected to Aggregators or Gateways. The operator side of the M2M network for health connects the Gateways to the Medical platform.

The Field area (Device to Gateway) connectivity varies for different area deployments. Example:

Area	Connectivity
Class 1	Fixed (USB etc) Wireless (BT, BLE, NFC, Wi-Fi, ZigBee, ANT etc)
Class 2	Fixed (USB etc.) Wireless (BT, BLE, NFC, Wi-Fi, ZigBee, ANT etc)
Class 3	Wireless

Table 3: Health Sector Field Area Connectivity

The Operator area (Gateway to Platform) connectivity has the following options.

Area	Connectivity
Class 1	Fixed (Ethernet, DSL) Wireless (3G etc)
Class 2	Fixed (Ethernet, DSL) Wireless (3G etc)
Class 3	Fixed (Ethernet, DSL etc.) Wireless (3G etc)

Table 4: Health Sector Operator Area Connectivity

4.3.3 Transport

The General M2M network architecture Model for transport vertical is illustrated in Figure 5.

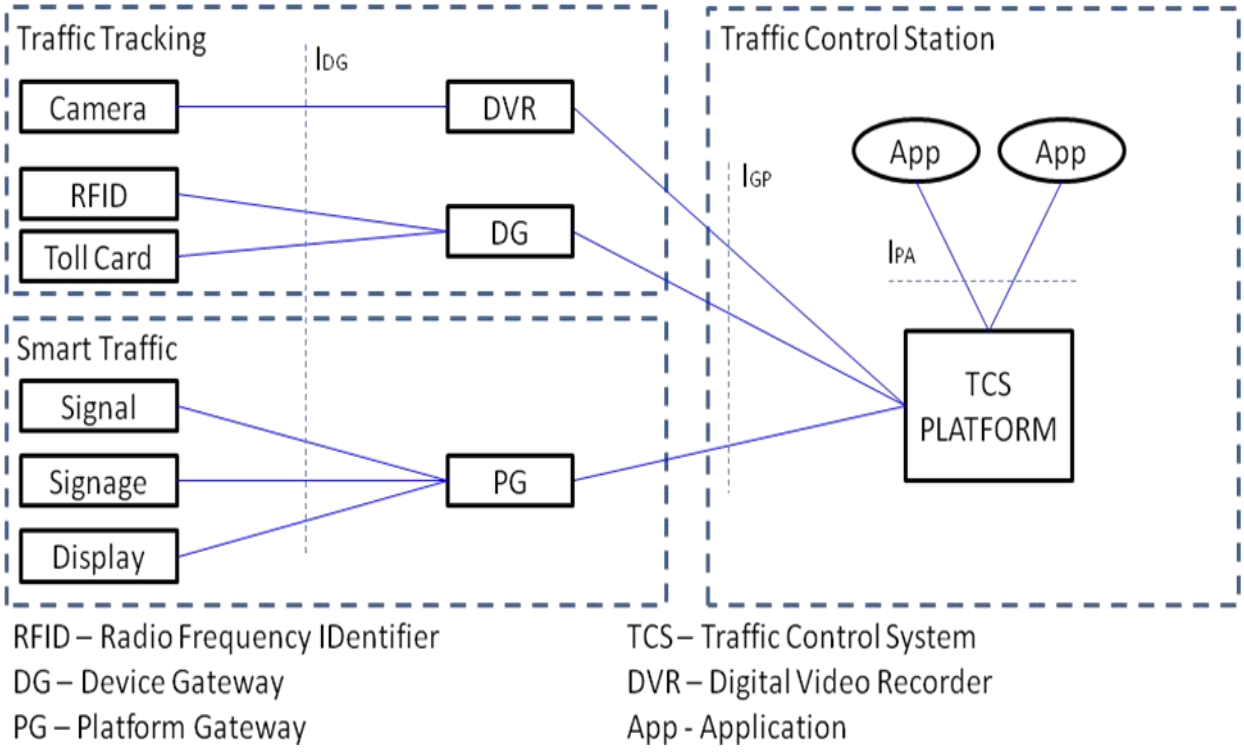


Figure 5: Transport Vertical M2M Network Architecture

The Field side of the M2M network for transport can be classified as Traffic Tracking and Smart Traffic. Traffic tracking consists of devices which sense vehicular and traffic data and push them to the control center through the gateways. The operator side of the M2M network for transport connects the Gateways to the Traffic controller platform.

The Field area (Device to Gateway) connectivity varies for different area deployments. Examples are:

Area	Connectivity
Traffic Tracking	Fixed (Ethernet over Optical, Ethernet) Wireless (RFID, NFC, DSRC etc)
Smart Traffic	Fixed (Ethernet over Optical, Ethernet) Wireless (2G,3G, WiFi, 802.11p etc.)

Table 5: Transport Sector Field Area Connectivity

The Operator area (Gateway to Platform) connectivity has the following options:

Area	Connectivity
Traffic Tracking	Fixed (Ethernet, etc.) Wireless (2G,3G, WiFi, 802.11p etc.)
Smart Traffic	Fixed (Ethernet, etc.) Wireless (2G,3G, WiFi, 802.11p etc.)

Table 6: Transport Sector Operator Area Connectivity

4.3.4 Safety and Surveillance

The M2M network architecture model for Safety and Surveillance (S&S) vertical is illustrated in Figure 6.

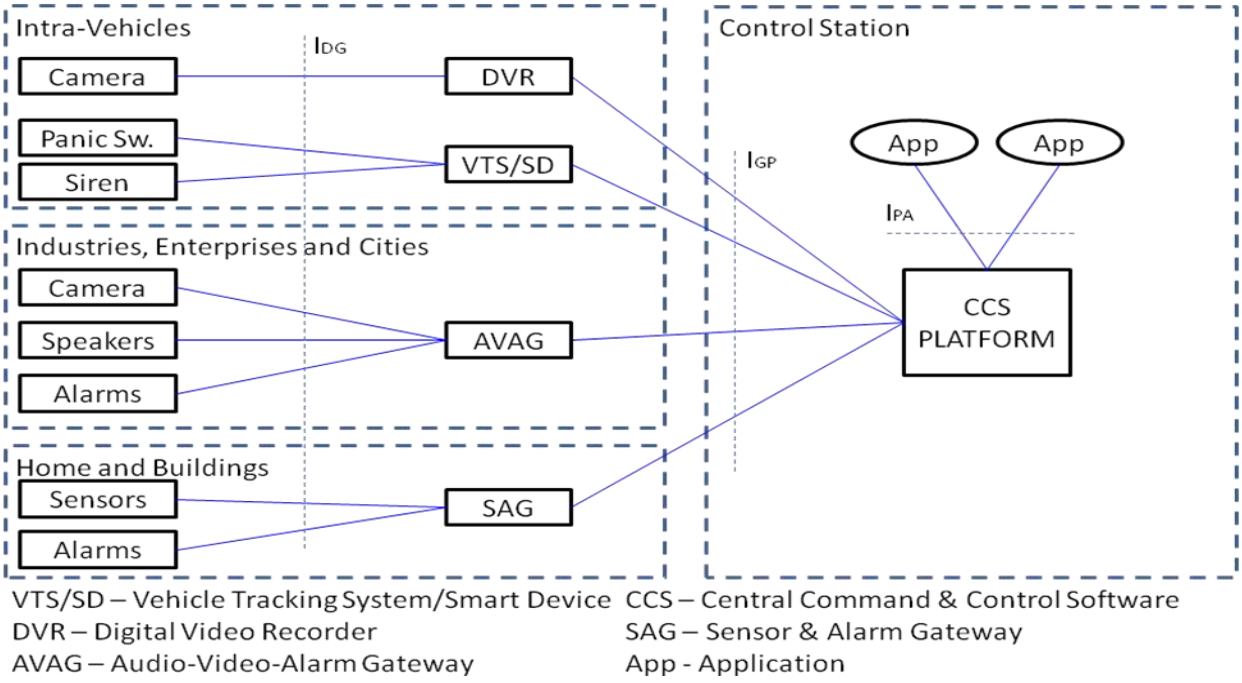


Figure 6: Safety & Surveillance Vertical M2M Network Architecture

The Field side of the M2M network for Safety & Surveillance(S&S) can be classified as:

i. **Intra-vehicle**: includes S&S sensors and gateways deployed for panic and monitoring;

ii. **Industries, Enterprises & Cities**: include S&S sensors and gateways for monitoring, disaster recovery etc.;

iii. **Home and Building**: which include S&S sensors and gateways for anti-theft, emergency services delivery, etc.

The Field area (Device to Gateway) connectivity varies for different area deployments. Example:

Area	Connectivity
Intra-Vehicles	Fixed (Ethernet etc.) Wireless (802.11p, Wi-Fi etc.)
Industries, Enterprises and Cities	Fixed (Ethernet) Wireless (2G, 3G, LTE, Wi-Fi, 802.11p Wi-Fi etc.)
Home and Buildings	Fixed (Ethernet, WPAN, BACnet, MODBUS etc.) Wireless (Wi-Fi, RFID, WPAN etc.)

Table 7: Safety and Surveillance Sector Field Area Connectivity

The Operator area (Gateway to Platform) connectivity has the following options.

Area	Connectivity
Intra-Vehicles	Fixed (Ethernet) Wireless (3G, Wi-Fi etc.)
Industries, Enterprises and Cities	Fixed (Ethernet over Optical etc.) Wireless (3G, Wi-Fi etc.)
Home and Buildings	Fixed (Ethernet over Optical, GPON, DSL etc.) Wireless (3G, 4G, Wi-Fi etc.)

Table 8: Safety and Surveillance Sector Operator Area Connectivity

4.4 Service Delivery Models

There are different models for M2M Service Delivery. The models suggested herein are primarily based on possible fragmentation and combination of various segments of the General Architecture Model. The names assigned to different service provider entities are for illustration purposes only and have no link with any category of existing or proposed service providers from licensing and regulatory angle. In Models 1 to 5 the illustrations are with one Service Provider for each sub layer. However, these 5 models also can be illustrated with multiple service providers in each sub layer. For illustration only four models i.e. Model 6 to Model 9 are shown with multiple Service Providers for each sub layer. Further, more than one model can co-exist. The terms used in the illustrations are E2ESP, FP, N&SP, PSP, M2M SP, ASP, and NSP.

4.4.1 Model 1: End to End M2M Service Provider

In this model, the End to End M2M Service Provider (E2ESP) provides and operates on the complete M2M ecosystem. The E2ESP shall provide the devices, gateways, the underlying network services, platform and applications. This is illustrated in Figure 7 below:

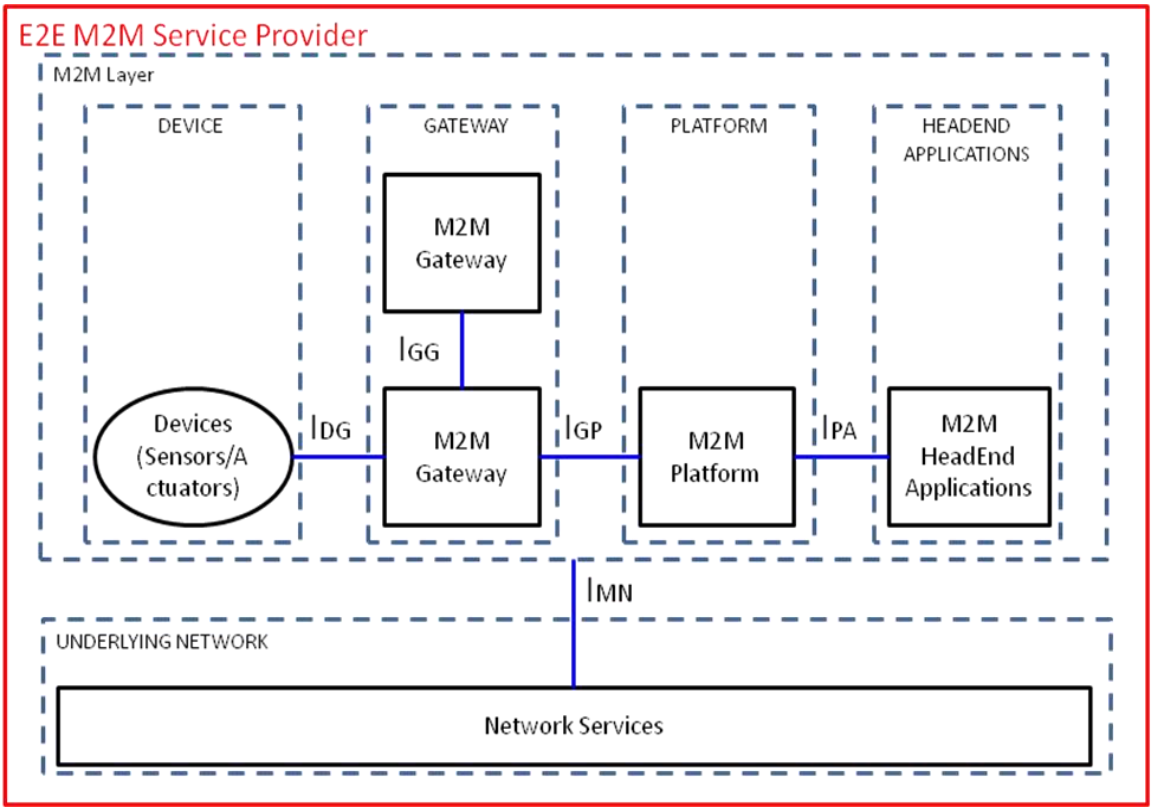


Figure 7: Model 1-M2M Network & Service Operator

4.4.2 Model 2: M2M Field Provider and M2M Network &Service Provider

In this model the Field Provider (FP) shall provide devices and gateways. The M2M Network and Service Provider (M2M N&SP) shall provide the underlying network services, platform and applications. The FP shall use the network services of the M2M N&SP for connecting devices to gateways and gateways to the platform. The M2M NSP shall provide common services to the FP. This is illustrated in Figure 8 below:

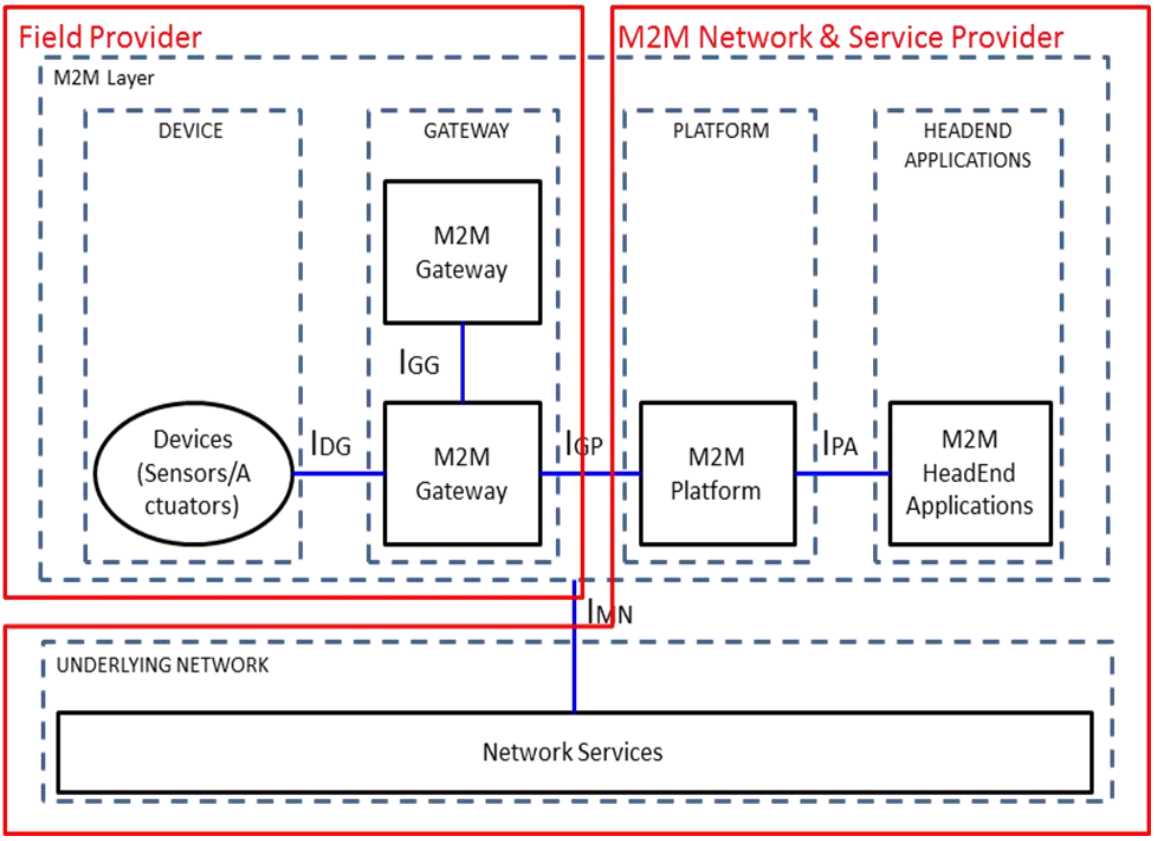


Figure 8: Model 2- M2M Field Provider and Network and Service Provider

4.4.3 Model 3: Field Provider, Network Service Provider and M2M Service Provider

In this model, the Field Provider (FP) shall provide devices and gateways, the M2M Service Provider (M2M SP) shall provide the platform and applications and the Network Service Provider (NSP) shall provide the network services. The FP shall use the network services of the NSP for connecting devices to gateways and gateways to the platform. The M2M SP shall provide the common services to FP. This is illustrated in Figure 9 below:

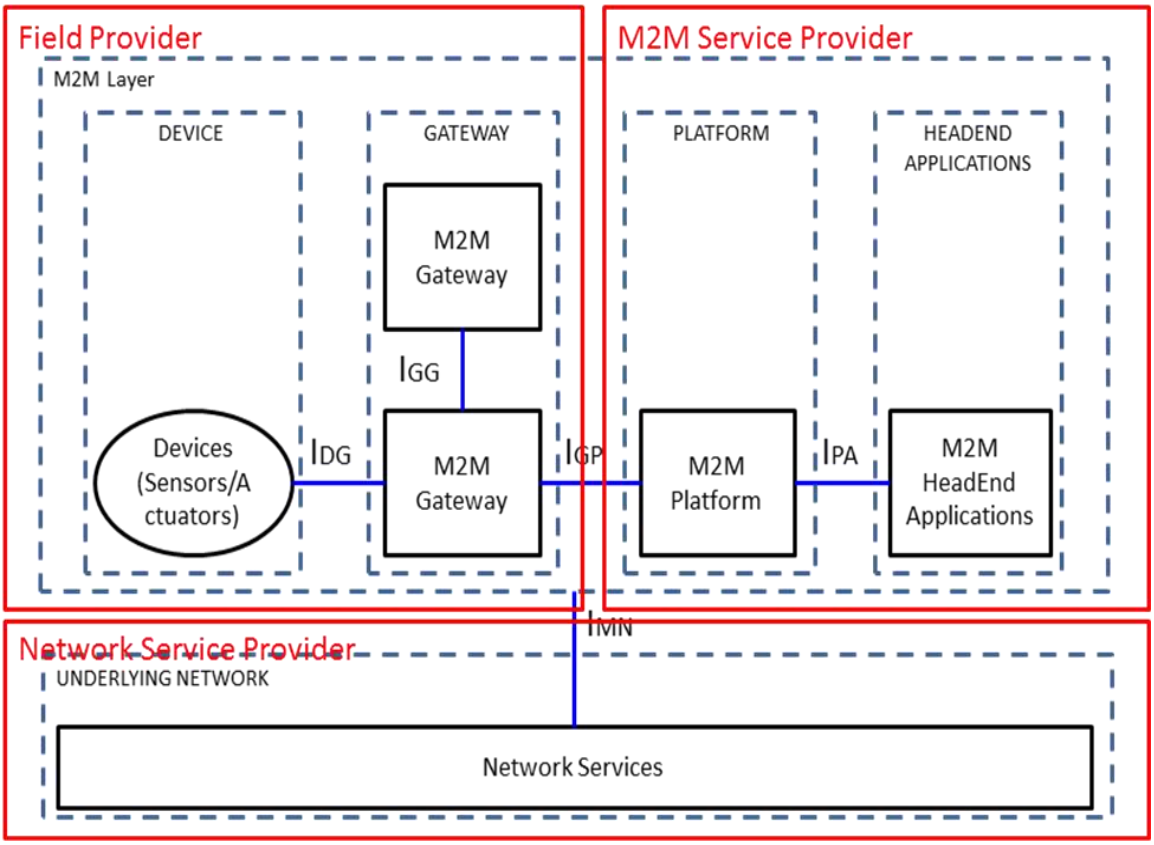


Figure 9: Model 3 - Field Provider, Network Service Provider and M2M Service Provider

4.4.4 Model 4: PAN operated Field Provider, Network Service Provider and M2M Service Provider

In this model, the Field Provider (FP) shall provide devices, gateways and also provides the PAN services. The PAN services allow connecting devices to gateways. The M2M Service Provider (M2M SP) shall provide the platform and applications and the Network Services Provider (NSP) shall provide the network services. The FP shall use the network services of the NSP for connecting gateways to the platform. The M2M SP shall provide the common services to FP. This is illustrated in Figure 10 below:

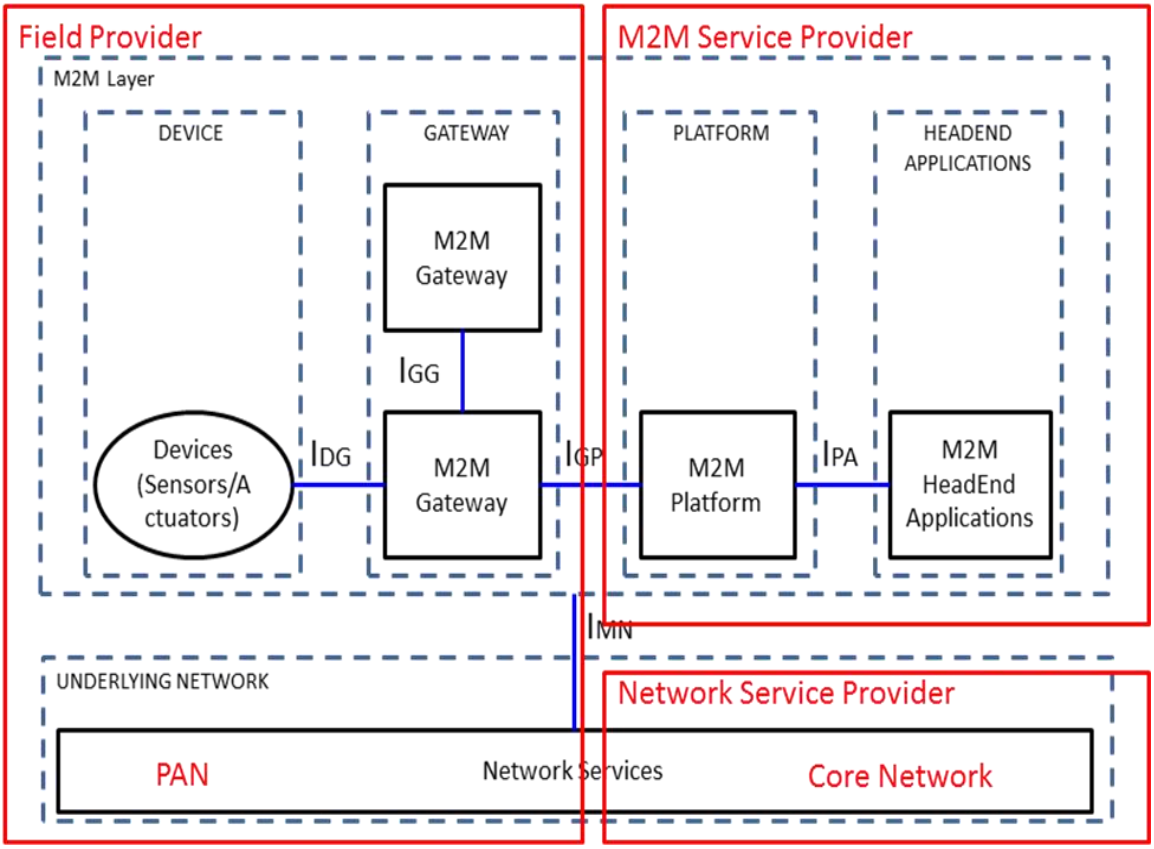


Figure 10: Model 4 - PAN operated Field Provider, Network Service Provider and M2M Service Provider

4.4.5 Model 5: M2M Field Provider, Platform Service Provider, Network Service Provider and Application Service Provider

In this model, the Application Service Provider (ASP) provides the applications for M2M verticals/industry. The Field Provider (FP) shall provide devices, gateways. The M2M Platform Service Provider (PSP) shall provide the platform. The Network Services Provider (NSP) shall provide the network services. The FP shall use the network services of the NSP for connecting devices to gateways and gateways to the platform. The ASP shall use the network services from NSP to connect applications to the platform. The PSP shall provide the common services to FP and ASP. This is illustrated in Figure 11 below:

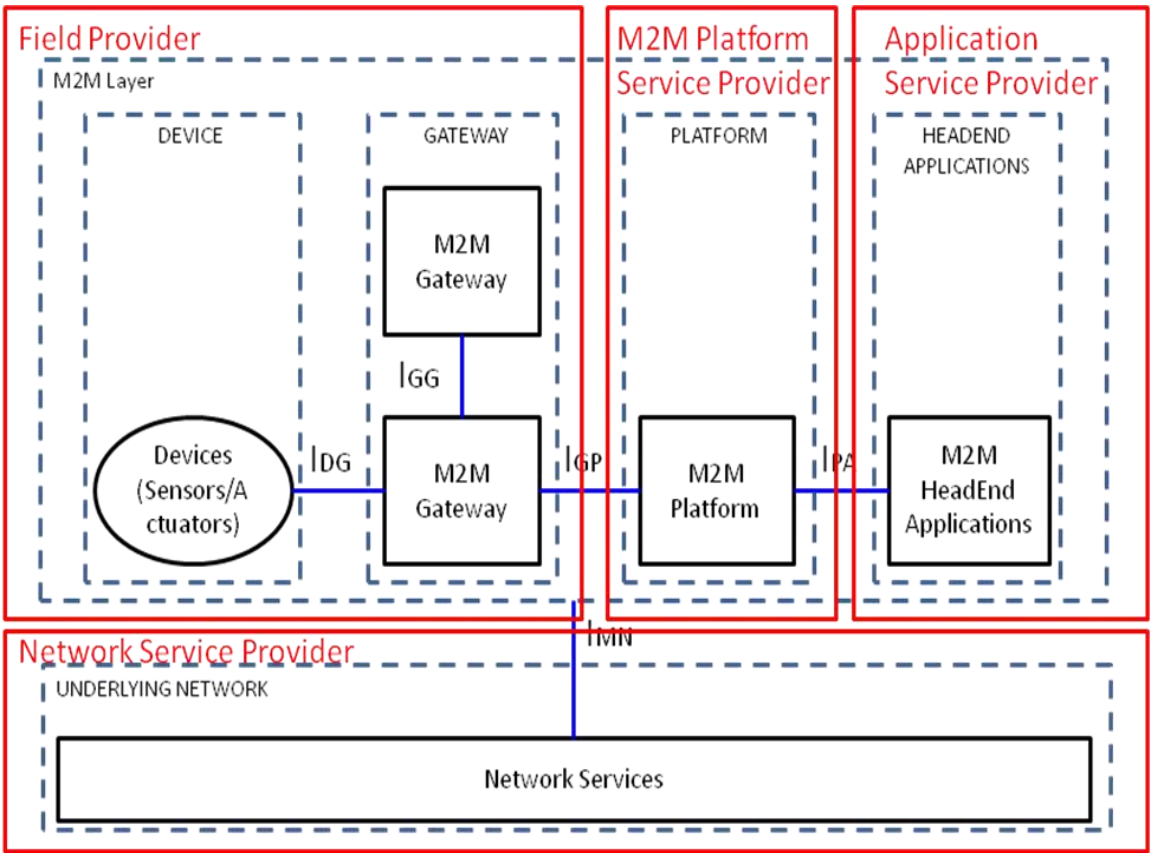


Figure 11: Model 5 - M2M Field Provider, Platform Service Provider, Network Service Provider and Application Service Provider

4.4.6 Model 6-M2M Field Provider, Platform Service Provider, Application Service Provider and Multiple M2M Network Service Providers

In this model, there can be multiple Network Service Providers (NSP). The Field Provider (FP) shall provide devices, gateways. The M2M Platform Service Provider (PSP) shall provide the platform. The Network Services Provider (NSP) shall provide the network services. The Application Service Provider (ASP) provides the applications for M2M vertical/industry. The FP shall use the network services of the NSP 1 for connecting devices to gateways. The FP shall use the network services of the NSP 2 for connecting gateways to the platform. The ASP shall use the network services (LAN/WAN) from NSP 3 to connect applications to the platform. The PSP shall provide the common services to FP and ASP. This is illustrated in Figure 12 below:

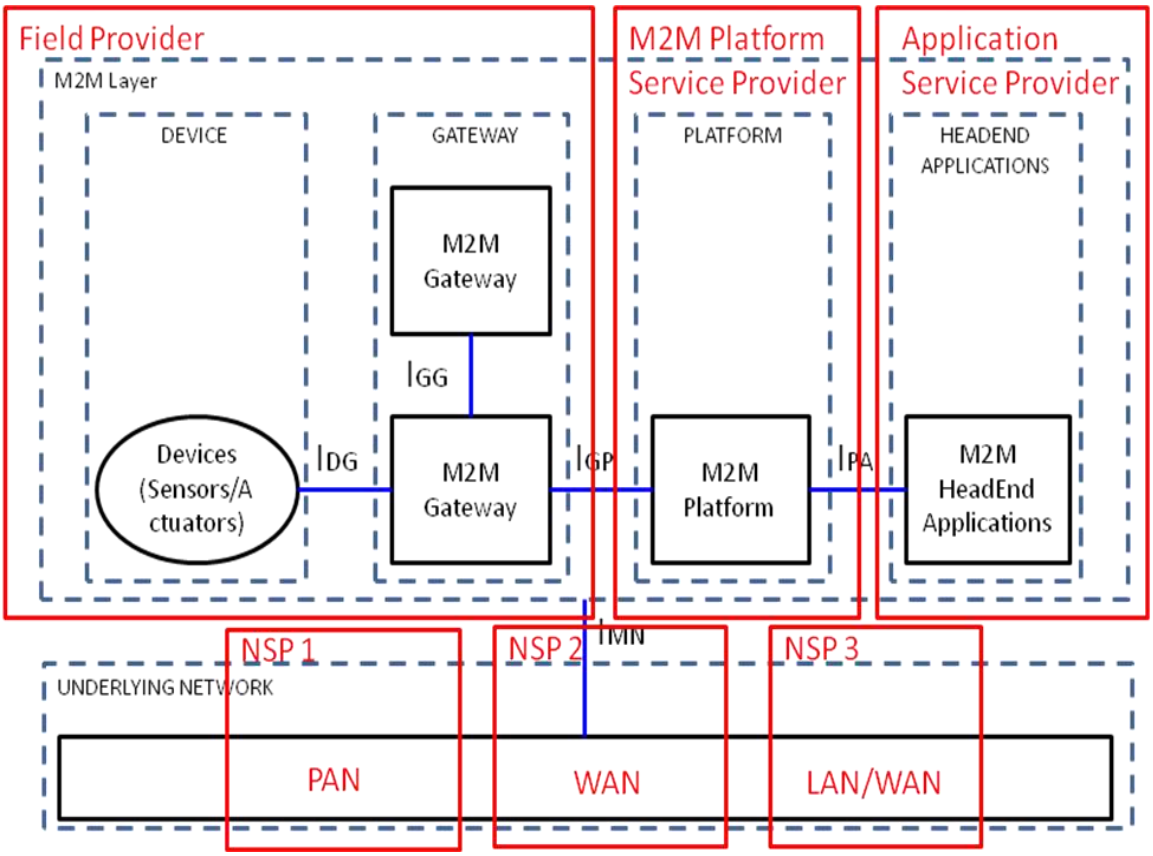


Figure 12: Model 6- M2M Field Provider, Platform Service Provider, Application Service Provider and Multiple M2M Network Service Providers

4.4.7 Model 7: M2M Field Provider, Application Service Provider, Network Service Provider and Multiple M2M Platform Service Providers

In this model, there can be multiple M2M Platform Service Providers (PSP). The Field Provider (FP) shall provide devices, gateways. The Network Services Provider (NSP) shall provide the network services. The M2M Platform Service Provider (PSP) shall provide the platform. The Application Service Provider (ASP) provides the applications for M2M verticals/industry. The FP shall use common services of M2M PSP2. The M2M PSP2 can use the common services of M2M PSP1 for enabling advanced application support. The ASP shall use the common services from M2M PSP2. The ASP may also use the common services from M2M PSP1. This is illustrated in Figure 13 below:

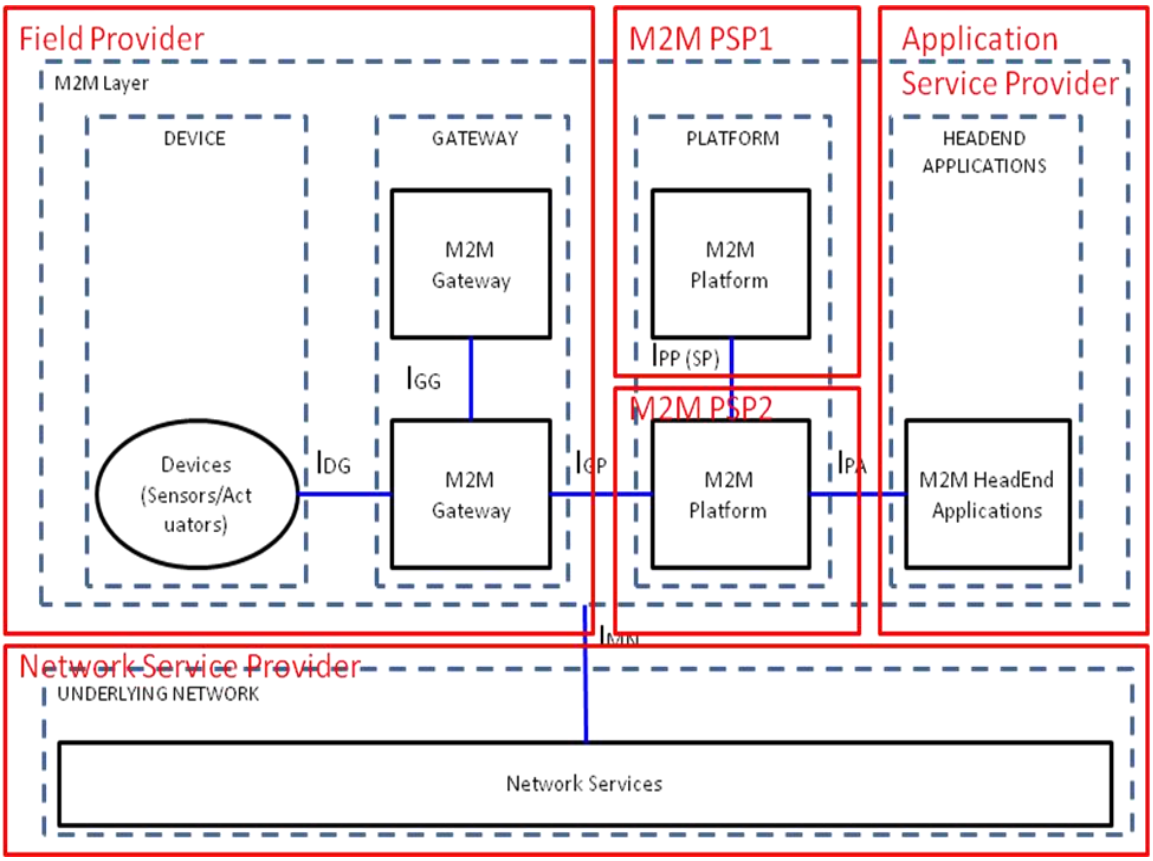


Figure 13: Model 7- Multiple M2M Service Providers over Common Network Service Provider

4.4.8 Model 8: M2M Application Service Provider, Network Service Provider ,Platform Service Provider and multiple M2M Field Providers

In this model, there can be multiple M2M Field Providers (FP). The Field Provider (FP) shall provide devices, gateways. The Network Services Provider (NSP) shall provide the network services. The M2M Platform Service Provider (PSP) shall provide the platform. The Application Service Provider (ASP) provides the applications for M2M verticals/industry. The FP1 and FP2 shall use common services of PSP. The PSP shall provide common services to different FPs and the ASP. This is illustrated in Figure 14 below:

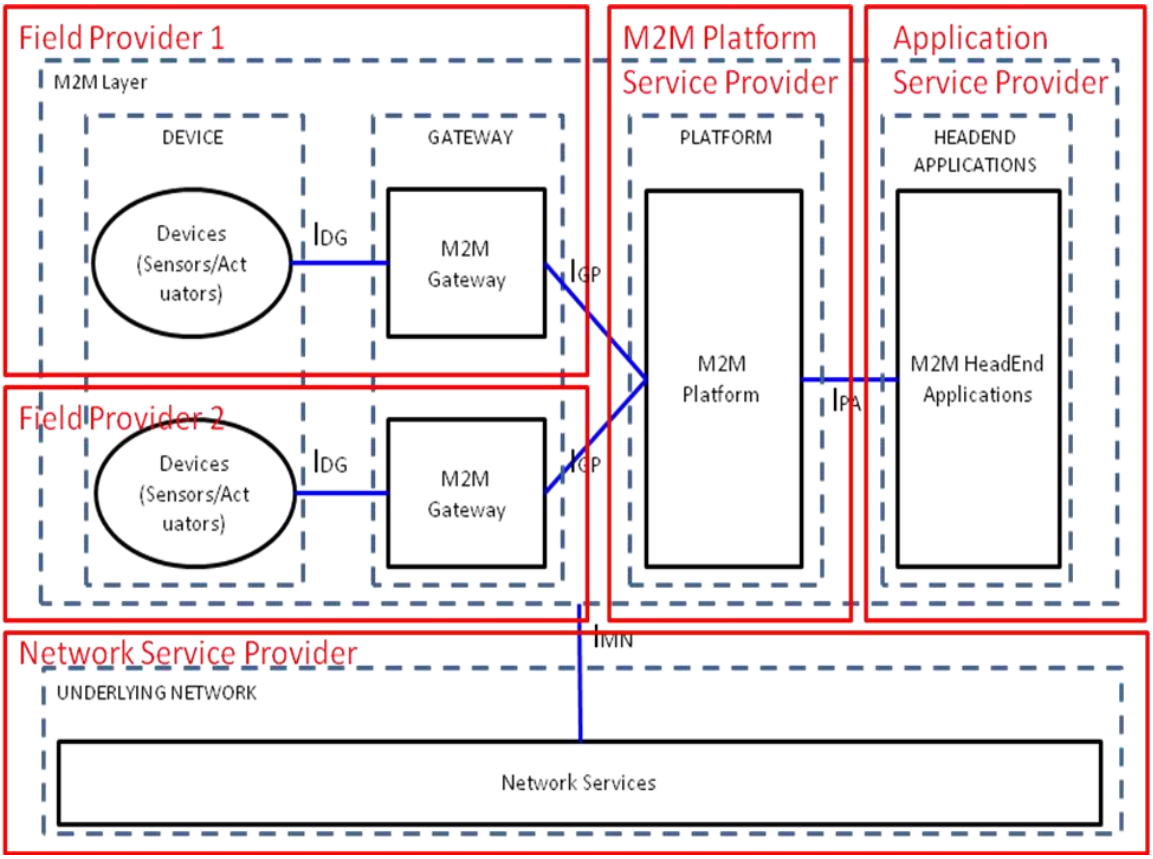


Figure 14: Model 8- M2M Application Service Provider, Network Service Provider, Platform Service Provider and multiple M2M Field Providers

4.4.9 Model 9: Hybrid M2M Provider(Multiple Field Providers, Application Service Providers, Network Service Providers and Platform Service Providers)

In this model, there can be multiple Field Providers (FP), M2M Service Providers (M2M SP), M2M Platform Service Provider (PSP), Network Service Providers (NSP) and Application Service Providers (ASP). The FP shall provide devices and optionally the gateways. The M2M SP shall provide the Platforms and optionally the gateways. The FP, M2M SP, PSP and ASP can utilize diverse underlying networks from NSP1, NSP2 or NSP3. The ASPs can utilize the common services from M2M SP and M2M PSP. Thus this model provides a hybrid model for M2M ecosystem. This is illustrated in Figure 15 below:

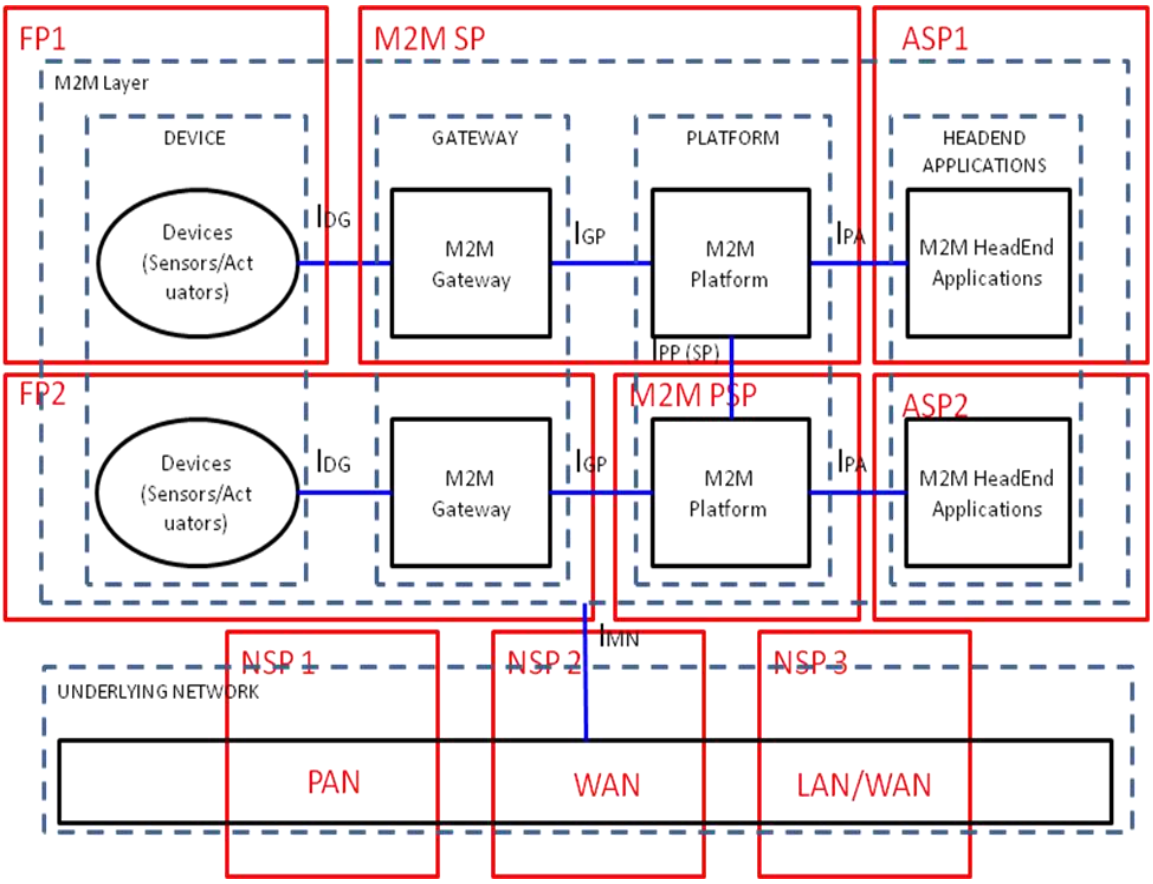


Figure 15: Model 9- Hybrid M2M Provider (Multiple Field Providers, Application Service Providers, Network Service Providers and Platform Service Providers)

4.5 Typical Applications of Service Delivery Models:

4.5.1 Power Sector

The most popular applications in the power sector currently being deployed as pilots are:

a) Advanced Metering Infrastructure (AMI)
b) Smart Grid Applications

The typical deployment scenario for AMI is illustrated in the Network Architecture Diagram (Figure 16) below:

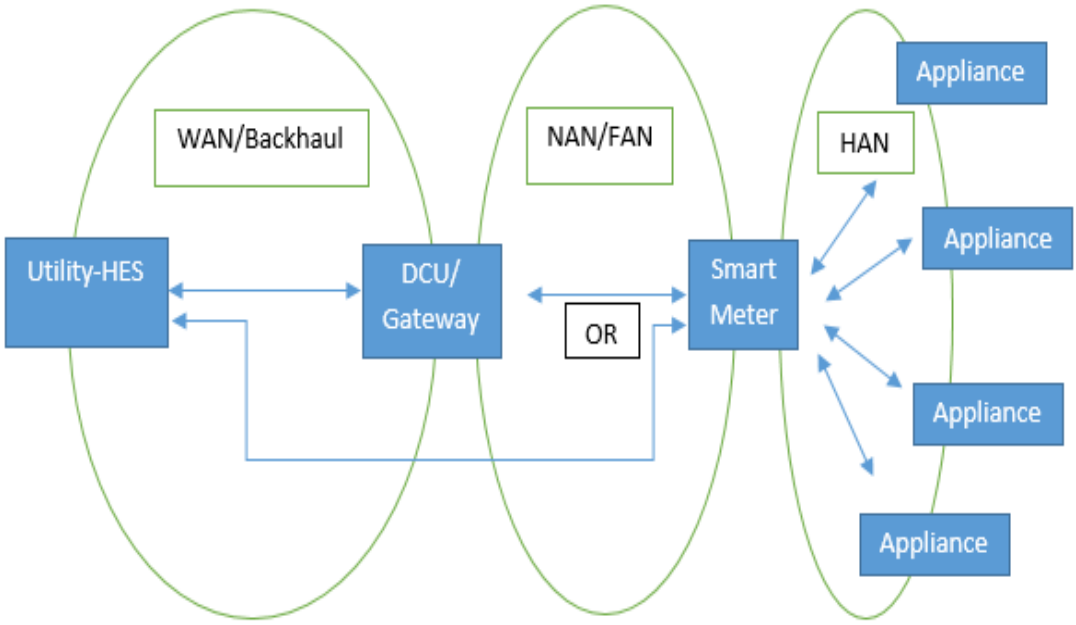


Figure 16: Typical Network Architecture for Advanced Metering Infrastructure (AMI) Application

The smart meters are connected to the DCU through NAN (Neighborhood Area Network)/FAN (Field Area Network) [For generality sake PAN would be used as the common TERM] which is further connected to the Utility Head End System through WAN/Backhaul. The various technologies used to connect the Meters to the DCU/Gateway are 6LowPAN, GPRS, PLC etc.

The most suitable service delivery model which can be mapped for such application is Model 4 i.e. PAN operated Field Provider, Network Service Provider and M2M Service Provider. In this model the meter supplier to the end user would also be taking care for the Personal Area Network, which may be 6LowPAN, Sub-GHz PAN, Wi-Fi or any other technology of choice suitable for the ergonomics/deployment scenario to connect to the DCU or Gateway. The backhaul can then be provided by a core Network Service Provider by means of MPLS, Optical Fiber, PLC, 3G, 4G, etc. The utility service provider (Power Distribution Company) may act as the M2M SP having the M2M Platform and also the Head-End Application.

Given below is the mapping of individual components to the ones illustrated in Service Delivery Model 4:

- Field Provider: Smart meter devices
- FAN: Personal Area Network with their own connectivity like 6LoWPAN, ZWave, ZigBee, etc.
- Gateway – Digital Connector/Concentrator Unit
- M2M Service Provider: utility Company providing the Automated Metering applications through the head end.
- Network Service Provider: WAN connectivity provider like GPRS, 2G,3G,4G or Wi-Fi services

Most of the models however are acceptable for deploying power vertical applications.

4.5.2 Transport

A typical Network Architecture Diagram is shown in Figure 17 below:

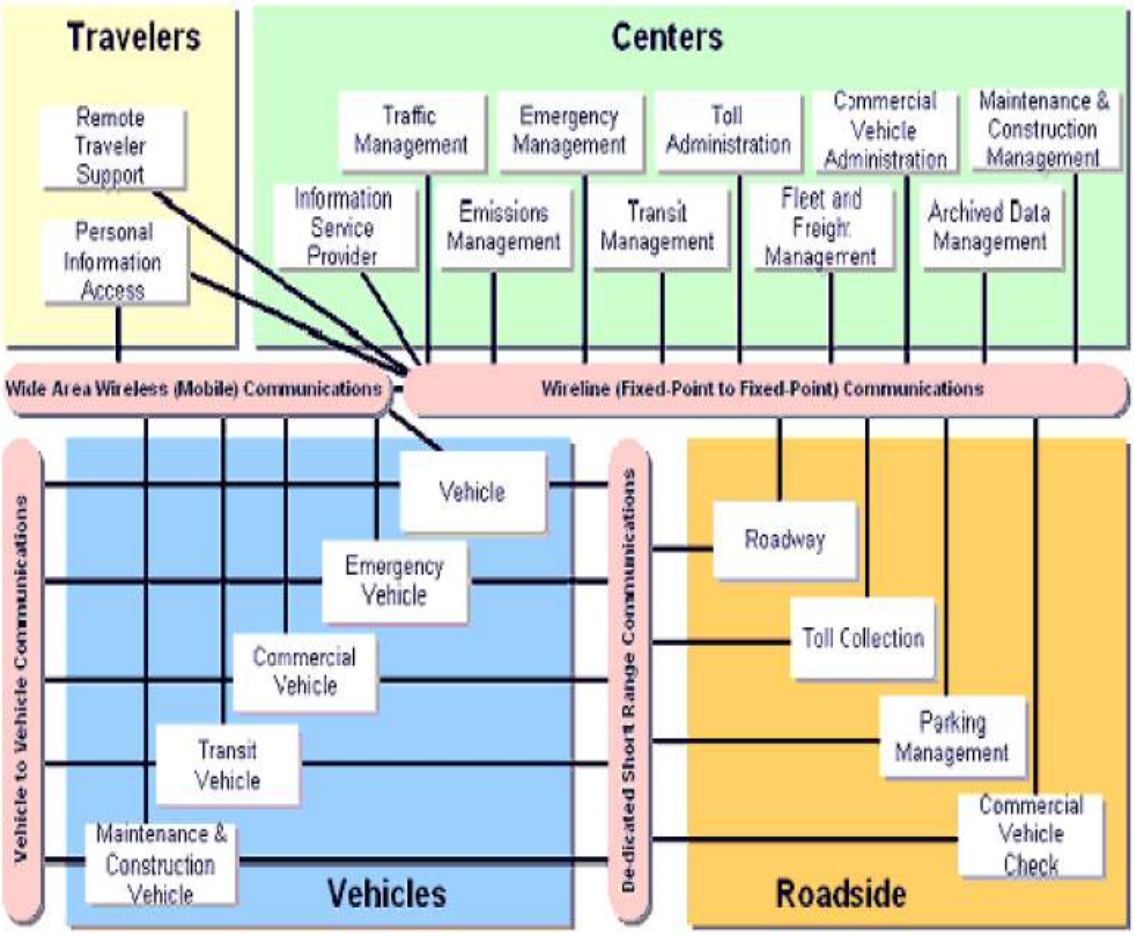


Figure 17: Intelligent Transport System Network Architecture

The Service Delivery Model suitable for the Intelligent Transport System is Model 3 - Field Provider, Network Service Provider and M2M Service Provider.

The devices in vehicles are deployed by the Field Provider, which connect to the Roadside gateways using Dedicated Short Range Communication (DSRC) technologies. These Gateways then connect to

the Center head end via WAN wireline networks and to the end users applications using WAN wireless networks.

Given below is the mapping of individual components to the ones illustrated in Service Delivery Model 3:

- Field Provider: Vehicle mounted devices like door sensors, fuel sensors, accelerometer, etc.
- Gateway – Toll collecting device, etc.
- M2M Service Provider: Centralized facility like Traffic management, etc.
- Network Service Provider: WAN connectivity provider like GPRS 2G,3G,4G or Wi-Fi services

4.5.3 Health

The typical deployment scenario for Tele health is illustrated in the Architecture Diagram (Figure 18) below:

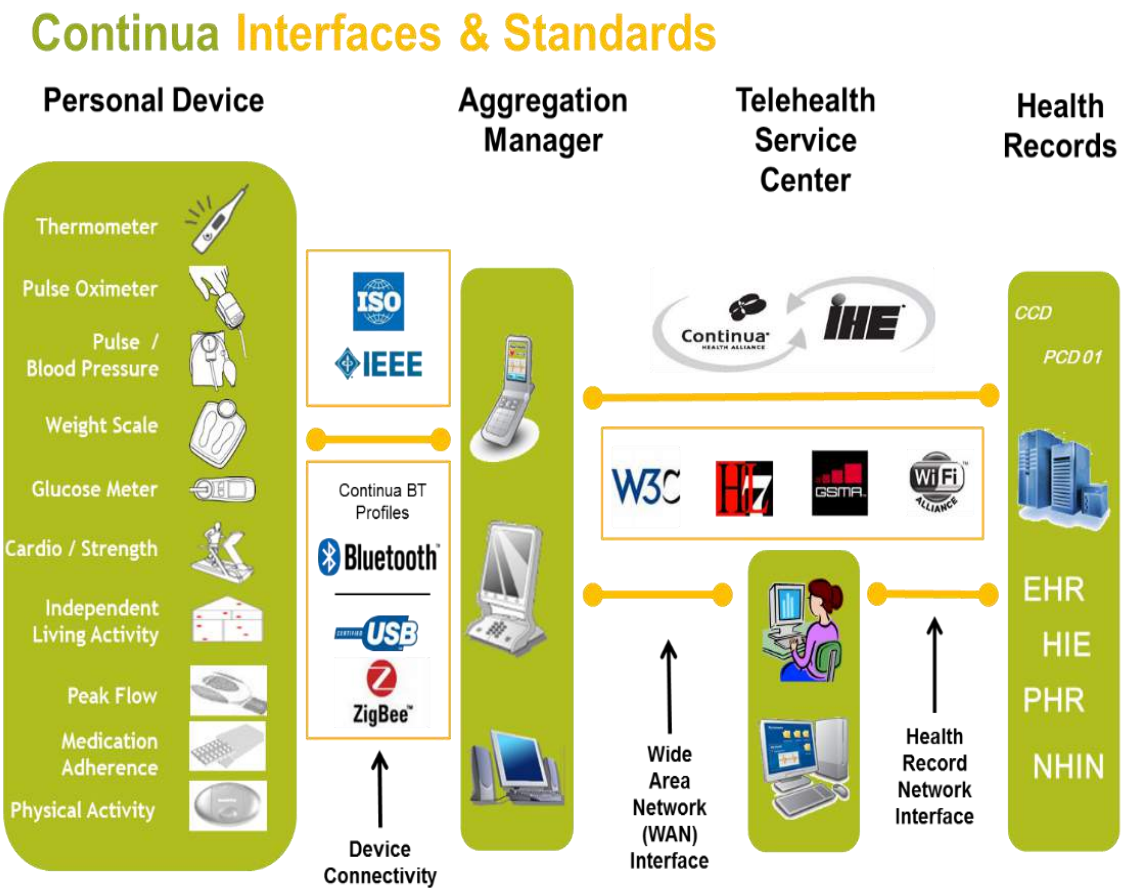


Figure 18: Continua Alliance Health Vertical M2M Network Architecture

Service Delivery Model 4 - PAN operated Field Provider, Network Service Provider and M2M Service Provider is suitable for the Health Vertical

The Health devices will operate in Personal Area Network with their own connectivity like BLE, ZigBee, NFC, etc. and communicate with Gateway over this connectivity. The gateway shall communicate with Cloud over the WAN connectivity.

The WAN connectivity is independent of the network provider. The data from the personal healthcare devices shall reach the Electronic Health Record system using the available network services. So, as per the Architecture diagram [Figure 18], the Field Provider (FP) shall provide devices, gateways and also provides the PAN services. The PAN services allow connecting devices to gateways.

Continua Alliance has followed H.810 design guidelines for the above which has also been approved by ITU.

Given below is the mapping of individual components to those illustrated in Service Delivery Model 4:

- Field Provider: Personal Healthcare devices for example Pulse-Oximeter
- PAN: Personal Area Network with their own connectivity like BLE, ZigBee, NFC, etc.
- Gateway – Smart Phone/Tablet, Dedicated Health gateway
- M2M Service Provider: Healthcare company providing the Electronic health record system
- Network Service Provider: WAN connectivity provider like GPRS 2G,3G,4G or Wi-Fi services

4.5.4 Safety and Surveillance

Safety and Surveillance can be implemented using the Service Delivery Model 1- End to End M2M Service Provider.

This can be used for Smart Phone/Tablet device based surveillance & Safety Solution. Wearable, Panic Button & Smart phone devices will fall into the device domain and Smart phone devices will themselves act as the Gateway also. The device will communicate with the gateway over Bluetooth connection. The gateway further will send the data to the Platform over 3G or Wi-Fi. The gateway can also use an alternative communication mechanism with the Platform and that could be SMS or over IVR, to inform the Platform, in case network connectivity is not available. Platform to application communications can be done over Wi-Fi, Fiber Optics, 3G and GSM, SMS.

Given below is the mapping of individual components of Safety & Surveillance to those illustrated in Service Delivery Model - Model 1:

- Device – Smart BLE Panic Button, Smart Phone/Tablet and other BLE wearable
- Gateway – Smart Phone/Tablet
- Platform – M2M Cloud
- Applications – Centralized NOC, Emergency service providers NOC, Patrolling Vehicle Applications etc.

4.6 Common M2M Service Layer Functional Architecture

Machine to Machine Communication is a very peculiar phenomenon because it requires so many disparate technology areas used in different verticals/industries to be brought together. However, the requirements for connectivity, security and data handling for all verticals/industries remain the same. However, vertical specific applications and solutions are likely to exist further. Therefore, collaboration is the only way to go in such scenario.

The main benefit of this collaboration will be much easier and cheaper to develop applications for any vertical, by reusing existing infrastructure, where applications can communicate with, cooperate with and reuse one another's data or components. A common Service Layer Architecture is therefore the way to go to achieve this. A standardized architecture with a common set of service layer capabilities and open interfaces and APIs should also help M2M providers to reduce investments, time-to-market, development and on-boarding costs, and facilitate management of devices and applications. This will help to build a solid M2M business case that relies on very small revenues, and even smaller margins.

4.7 About OneM2M

OneM2M is the leading global standardization body for M2M. It was established through an alliance of standards organizations to develop a single horizontal platform for the exchange and sharing of data among all applications. OneM2M is creating a distributed software layer – like an operating system – which is facilitating that unification by providing a framework for interworking with different technologies. Those are the two key elements at the core of oneM2M: providing an interworking framework and enabling re-use of what is already available as much as possible.

4.7.1 oneM2M Functional Architecture Analysis

Figure 19 below illustrates the oneM2M functional architecture for the M2M service layer.

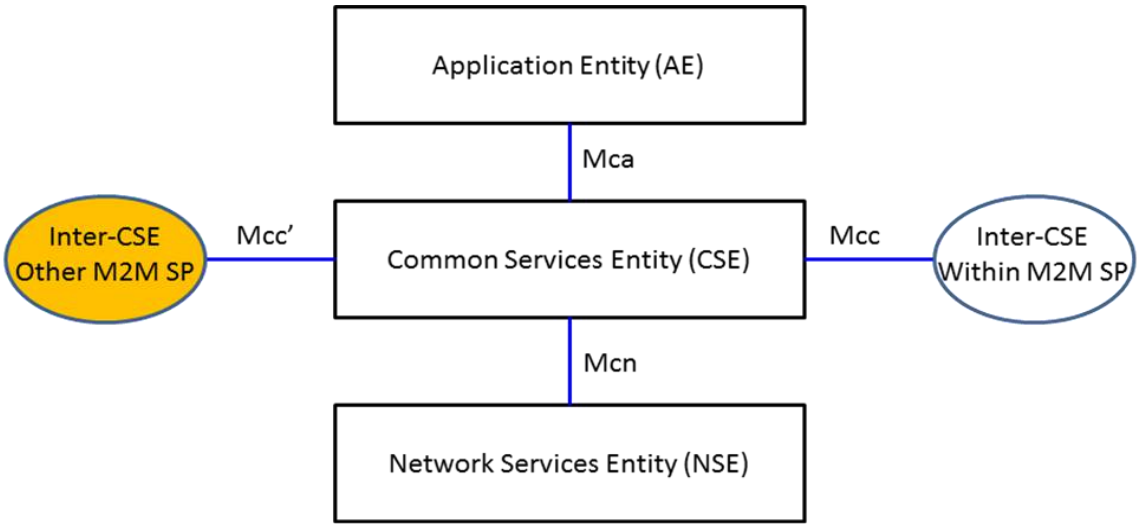


Figure 19: oneM2M Functional Architecture

The oneM2M functional architecture is based on Internet Protocol. It consists of the following entities:

- Application Entity (AE): It is responsible for the application service logic. E.g. health monitoring, power meter reading, etc. An application can be composed of multiple AEs distributed in different nodes in the M2M network. Each AE instance is uniquely identified using an Application Entity ID (AE-ID). It relies on the CSE for realizing end to end application support services like communication, addressability, etc.
- Common Services Entity (CSE): It is responsible for providing the Common Service Functions (CSFs) to the AEs and the other CSEs. CSE is the key entity for realizing the "common" part for different verticals/industries. One CSE can be constituted of varying number of CSFs thus enabling CSE distribution in hierarchical mode. One CSE shall support multiple AEs (from same or different verticals). Multiple CSEs can be distributed in different nodes in the M2M network to support ease of application development and deployment. Each CSE instance is uniquely identified using a Common Services Entity ID (CSE-ID). It may utilize some underlying network services functions for network dependent functionality of the device like location, wakeup, etc. Hence it may provide some underlying network gateway functions like protocol conversion, etc.
- Network Services Entity (NSE): It is responsible for providing the special network services to the CSE e.g. Location service, Device management, device triggering, etc. This network related capabilities allow CSEs to provide more intelligent support to application interactions.

4.7.2 Reference Points and Interfaces

The following are the reference points for the oneM2M functional architecture:

- Mca: This reference point provides the bi-directional communication among AE and CSE within a M2M Service Provider (M2M SP). This communication interface is IP-based. The service interface is based on REST principles.
- Mcc: This reference point provides the bi-directional communication between the distributed CSEs within a M2M Service Provider (M2M SP). Mcc allows scaling of the common services within the M2M SP. This communication interface is IP-based. The service interface is based on REST principles.
- Mcn: This reference point provides the bi-directional communication between CSE and NSE to use the network supported services apart from transport and connectivity (which is implicit to this architecture). This communication uses the underlying network protocol and interface e.g. 3GPP, etc.
- Mcc': This reference point provides the bi-directional communication between CSEs from different M2M Service Providers (M2M SPs). Mcc' allows scaling the Mcc reference for requesting common services across M2M SPs. This communication interface is IP-based. The service interface is based on REST principles.

Other reference points that are not defined in the current version:

- Mch: This reference point provides the bi-directional communication of CDRs between CSE and the Charging Server. This communication uses the underlying network protocol and interface e.g. 3GPP defined Rf.

4.7.3 oneM2M Common Service Functions

The Common Service Functions (CSF) defined in oneM2M is specified for informative purpose, they are not yet standardized. There is no limitation on CSE towards the constitution of CSFs. As the name suggests, the CSFs should be commonly used by most vertical/industry applications. The following list of CSFs is currently supported in oneM2M Release 1.0:

a. Application and Service Layer Management
b. Communication Management and Delivery Handling
c. Data Management and Repository
d. Device Management
e. Discovery
f. Group Management
g. Location
h. Network Service Exposure, Service Execution and Triggering
i. Registration
j. Security
k. Service Charging and Accounting
l. Subscription and Notification

4.7.4 M2M Systems Analysis

The M2M network models described in section 3.4 can be realized using the oneM2M functional entities by distributing them to different physical nodes in each M2M domain:

a. **Device Nodes:** There is a wide diversity in the architecture of the device nodes which support different verticals/industries. It allows definition for a simple sensor device to an intelligent sensor device. The current version of oneM2M system/node descriptions defines the following types of device nodes :

   i. ***Non-oneM2M Low Capability Devices (NO-LCD)***: These devices require support of an Interworking Proxy Entity, which shall provide for Non-oneM2M interfaces. This is characterized by data model translation into M2M data model, protocol translation, etc.

ii. ***Low Capability Device (LCD):*** This device is referred as "Application Dedicated Node" in oneM2M system. This node comprises of at least one AE. It communicates with CSE of Gateway and Platform Nodes using Mca.

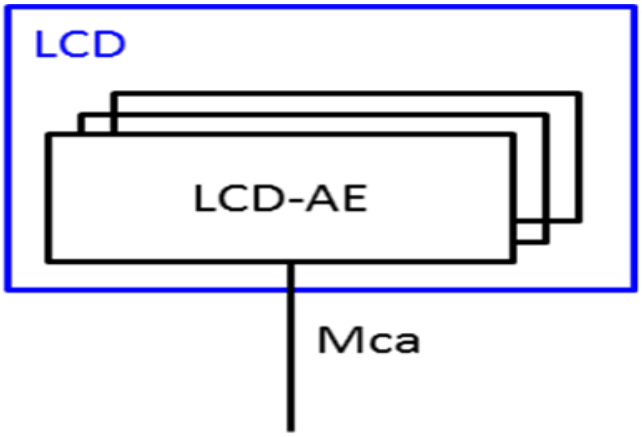


Figure 20: Low Capability Device

If the LCD is not an oneM2M compliant device, it is able to communicate within an oneM2M system using ASN and MN nodes which are oneM2M compliant. The ASN or MN or IN nodes can host the proxy functions to the non-oneM2M LCD.

iii. ***High Capability Device (HCD)***: This device is referred to as "Application Service Node" in oneM2M system. This node comprises of at least one AE and one CSE. The AE communicates with CSE on the same node using Mca. The CSE communicates with CSEs of Gateway and Platform nodes using Mcc. The CSE communicates with the underlying network using Mcn.

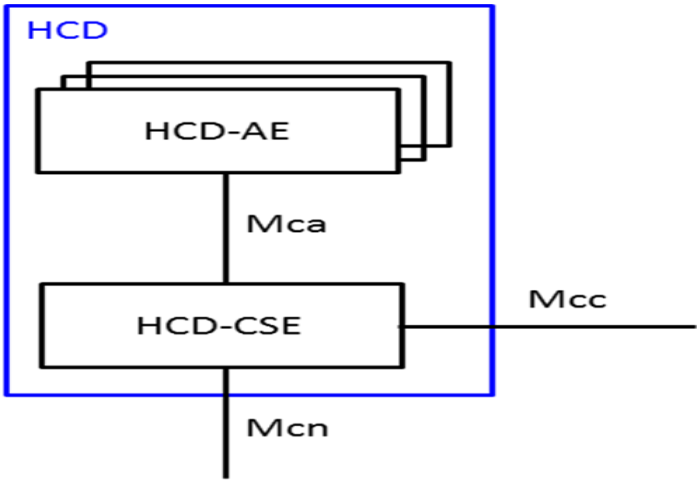


Figure 21: High Capability Device

Note: For HCD device nodes, the capability to use Mcc' is FOR FURTHER STUDY.

iv. **Gateway Nodes:** This gateway functions can be realized using the "Application Service Nodes" and "Middle Nodes" in oneM2M system. This ASN comprises of at least one AE and one CSE, while the MN comprises of at least one CSE and optionally an AE. The AE

communicates with CSE on the same node using Mca. The CSE communicates with AE of Device nodes (LCD, HCD) through Mca and with CSE of Platform nodes through Mcc. The CSE communicates with the underlying network using Mcn. When the device nodes are not oneM2M compliant, the Gateway AE will perform the proxy AE functions for the non-oneM2M devices.

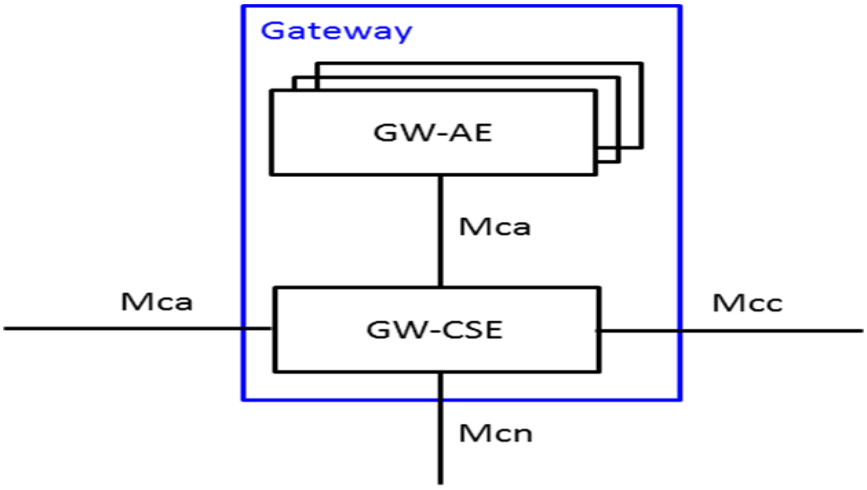


Figure 22: Gateway Node

Note: For Gateway nodes, the capability to use Mcc' is FOR FURTHER STUDY.

v. **Platform Nodes:** These nodes are referred to as "Infrastructure Nodes" in oneM2M system. It comprises of at least one CSE and optionally an AE. The AE communicates with CSE on the same node using Mca. The CSE communicates with AE of Device nodes (LCD, HCD) and Gateway nodes through Mca. For geo-distribution of the platform CSEs by a M2M SP the CSE may communicate with CSE of another platform node through Mcc (This aspect is FOR FURTHER STUDY). The CSE communicates with other M2M SP Platform Nodes' CSE through Mcc'. The CSE communicates with the underlying network using Mcn.

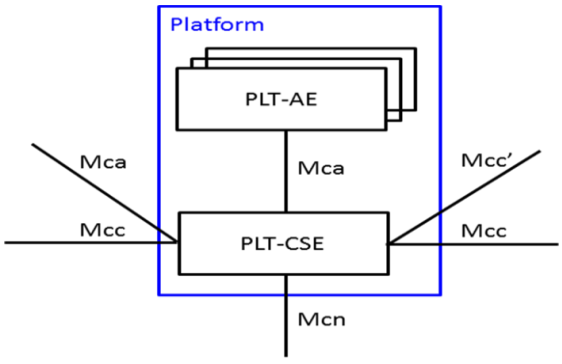


Figure 23: Platform Node

Application Nodes: These nodes are responsible for the end user aspects of the M2M application. The end user parts of the application may use different capability execution platforms e.g. handheld devices or Servers. Hence Application Nodes can further be classified as:

i. ***Application User Equipment Node (AUE):*** This node may comprise of oneM2M AE. The AE communicates to the CSE of Platform Node through Mca.

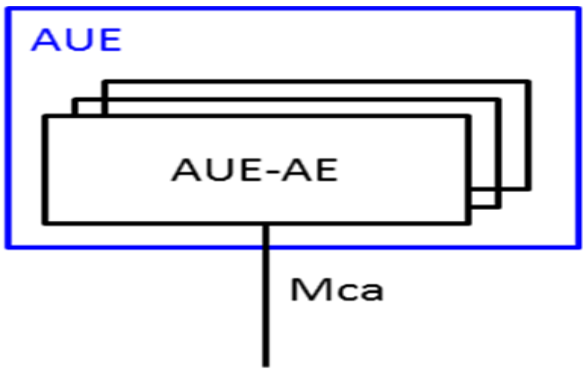


Figure 24: Application User Equipment Node

Application Server Node (AS): This node comprises of at least one AE and one CSE. The AE communicates to the CSE through Mca. The CSE communicates with the CSE of Platform Node through Mcc.

Note: For AS nodes, the capability to use Mcc', Mcn is FOR FURTHER STUDY.

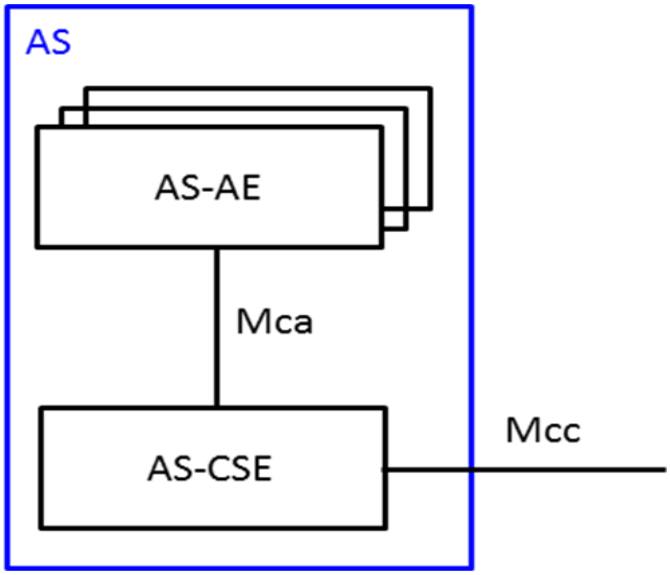


Figure 25: Application Server Node

Example: An end to end M2M system for Smart Home and another application leveraging the common oneM2M functions is illustrated in Figure 26 below:

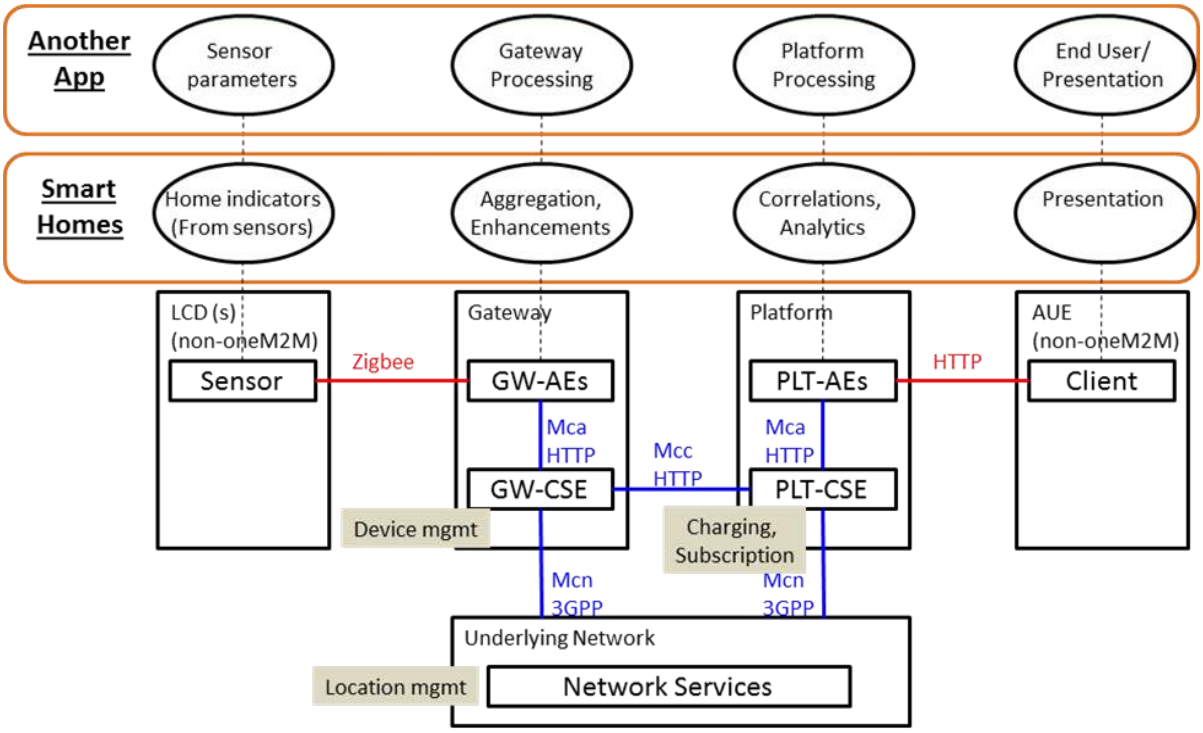


Figure 26: Example E2E M2M System

A smart home application will consists of variety of sensors such as for temperature, for electrical devices' status etc. The gateway is also usually deployed in the home environment. All the sensors communicate to the gateway using protocols like ZigBee. The Gateway in this case shall provide a proxy application (GW-AE) to convert the ZigBee protocol from device side to the common protocol like HTTP on the gateway side (GW-CSE). It may also offer application side processing elements for enhancing the sensor aggregated information. The gateway (GW-CSE) offers device management and self-organizing functions to allow elastic scaling of sensors in the home environment. The Gateway connects to the Platform over IP network. The common services residing on the Gateway (GW-CSE) communicates with the Platform service (PLT-CSE) using HTTP/CoAP/MQTT protocols. The platform offers subscription, security and charging services to develop the applications for smart home. The Platform services (PLT-CSE) communicates with the application part using HTTP protocol. The application part of the Platform (PLT-AE) may provide application functions like Analytics, Correlation and presentation support functions. These functions can be accessed by the User Equipment Client (e.g. Browser) from the Platform application part using HTTP protocol. The Gateway and Platform may use an underlying network for advanced device information services like Location, Device Triggering, Charging, etc. to enhance the common services provided to the application part.

In the above example, the gateway and platform are oneM2M compliant. The sensors and end user equipment use non-oneM2M interfaces to communicate with the gateway and platform respectively.

4.7.5 Mapping Generic M2M Network Architecture Models with oneM2M Architecture

The following table illustrates the mapping of the Generic M2M Network Architecture model with oneM2M Architecture

Sl.	Generic M2M Network Architecture Model	oneM2M Architecture
Domains		
1	Device Domain	Part of Field Domain
2	Gateway Domain	Part of Field Domain
3	Platform Domain	Part of Infrastructure Domain
4	Application Domain	Part of Field and Infrastructure Domain
Systems		
5	Low Capability Device (LCD) Node	Application Dedicated Node (ADN)
6	High Capability Device (HCD) Node	Application Service Node (ASN)
7	Gateway Node	Middle Node
8	Platform Node	Infrastructure Node
9	Application User Equipment (AUE) Node	AE part of Infrastructure Node acts like the Server part.
10	Application Server	AE part of Infrastructure Node Application Server itself is out of scope
Physical Interfaces		
11	I_{DG}	Mca (AE-CSE) Mcc (CSE-CSE) Supports PAN protocols (Out of Scope)
12	I_{GP}	Mcc (CSE-CSE)
13	I_{GG}	Mcc (CSE-CSE)
14	I_{PA}	Mca (CSE-AE)
15	I_{PP}	Mcc (CSE-CSE)
16	$I_{PP\ (SP)}$	Mcc' (SP1 CSE- SP2 CSE)
17	I_{MN}	Mcn (CSE-NSE) Mch (CSE-3GPP Charging Server) Extensible to other Protocols like OMA, BBF, etc.
Business Entities		
18	Field Provider containing Device Nodes (LCD, HCD), Gateway nodes	M2M Service Provider – Field Domain containing multiple ADN, ASN, MN, non-OneM2M Devices
19	M2M Service Provider containing Device Nodes (LCD, HCD), Gateway nodes, Platform nodes, application nodes (AUE, AS)	M2M Service Provider – Infrastructure Domain (supports only one IN) – Does not include the Application Server
20	Application Service Provider containing application nodes (AUE, AS)	Application Service Provider – Out of Scope
21	Network Service Provider	Network Service Provider – Out of Scope

Table 9: Mapping of Generic M2M Network Architecture with oneM2M

4.8 M2M Architecture Common Aspects

4.8.1 Naming and Addressing

The naming scheme in M2M architecture shall define the identifiers for the M2M entities (applications, resources, nodes, network related, etc.) like URI, E.164, etc. The identifiers should allow device management without human intervention. The addressing scheme for M2M shall define the reachability mechanism for any application and services in the devices, gateways,

platforms and head end applications. Various addressing schemes can be adopted to enable the reachability to any entity in the M2M realm. E.g. IP, SIM, etc.

OneM2M also specifies M2M Identifiers and Resource addressing mechanisms [4] for M2M communication. Detailed analysis and recommendation of M2M Naming and Addressing not in the scope of this document and will be captured as a separate technical report.

4.8.2 Communication

The communication to the M2M Gateway is of critical importance as it forms the back-bone of M2M systems. The main factors for consideration are:

- Reliability
- Cost
- Manageability
- Accuracy
- Security

The reliability of communication media depends upon geography, climatic conditions, wiring condition and topography i.e. urban or rural. A communication channel maybe provided through guided media such as copper/ optical fiber cable or through an unguided medium such as radio link. The performance of a communication channel is mainly characterized by the following parameters:

- Bandwidth/ bit rate
- Attenuation
- Noise
- Signal processing delay

Both wired and wireless communication technologies can be considered for M2M Gateways. In certain situations, wireless technologies have advantages over wired technologies, such as low cost and ease of connection but disadvantages are interference & signal attenuation. Wired communication are more reliable, less prone to interference but very expensive to deploy.

The Service Layer Communication in M2M system shall be IP based:

- IPv4 – Limited address space for M2M applications.
- IPv6
    - 128 bit addressing scheme and supports virtually unlimited number of devices- 340 trillion trillion. – Very highly scalable
    - In-built IPsec – Authenticates and encrypts each IP packet of a communication session

Different wireless, wireline communication technologies for M2M communications are discussed in Section5.

4.8.3 Security

Note: The security analysis of the general M2M Network Architecture and the deployment models considering oneM2M is FOR FURTHER STUDY.

The following general security requirements are applicable to M2M networks:

- **Availability**: Information network should be available for use of the concerned parties in the manner intended. This can be ensured by monitoring the network at device level, communication level and at the control centre end.
- **Authentication**: This should provide assurance that a party in data communication is who or what they claim to be.
- **Authorization**: This security service should ensure that a party may only perform the actions that they are allowed to perform.
- **Integrity:** Integrity should ensure that data/ information cannot be altered in an unauthorized or malicious manner. Architecture should include strong Point to point communication schemes to prevent spoofing and injection of false data.
- **Confidentiality**: Data and information should be protected from being disclosed to third party. Confidentiality of data and information is achieved by providing role based access at both data & information level and at device level

M2M infrastructure consists of measurement devices, gateway devices/ aggregators, communication network for information exchange and control centre to collect data & information and use it for the intended operations. Information is exchanged at device level where it is generated, during exchange on the communication network and at control centre where it is collected for intended use.

The architecture will include measures to ensure security of data at different modes like security for systems, communications and also service provider/operations.

Detailed analysis and recommendation of M2M security is not in the scope of this document and will be captured as a separate technical report.

5. Requirements Analysis for M2M Standards

Important requirements from different Verticals are considered here. Requirement analysis with respect to existing Standards is illustrated as under. Topics of future Standards are included.

5.1 Wireless - Spectrum and Radio Standards

S. No.	Frequency Band	Radio Technology	Verticals	Related Standards	Remarks
1	2.4 GHz	Bluetooth	• Health • Power • Safety & Surveillance	IEEE 802.15.1	-Need higher data security -Prone to interference
2	3.1 GHz – 10.6 GHz	UWB	• Health • Power	IEEE 802.15.3a	-Spectrum allocation is required. -Use as is
3	2.4 GHz	ANT[1]	Health	Proprietary by Dynastream Innovations Inc.	-Use as is
4	780 MHz 868 MHz 915 MHz 920 MHz 2.4 GHz	ZigBee	• Health • Power • Safety & Surveillance	IEEE 802.15.4	-Low reliability -High Stack size -High power consumption -Uncertain radio connectivity
5	2.4 GHz 5 GHz	Wi-Fi	• Health • Power • Safety & Surveillance	IEEE 802.11a/b/g	-High Interference -High power consumption
6	>300 GHz	Infrared	• Power • Transport	IrDA[2] ISO/DIS 21214	-Line of sight
7	13.56 MHz	NFC	• Health • Power • Transport	ISO/IEC 18092/21481	-Low information security
8	100 KHz – 10 GHz	RFID	• Health • Power • Transport	ISO 14443[3] (13.56 MHz)	-Connectivity can be hampered -Low data security

[1] http://www.thisisant.com/
[2] http://www.irda.org/
[3] http://wg8.de/

9	865 MHz – 956 MHz	Z-Wave	• Power • Safety & Surveillance	Z-Wave[4]	-Not very scalable -Unpredictable throughput and latency
10	TV Band	TVWS	• Power • Transport • Safety & Surveillance	IEEE 802.11af IEEE 802.22	-Dynamic allocation of TV frequency bands is complex -Regulation for Spectrum and other technical parameters is required. Technology under development
11	400 MHz 900 MHz 2.4 GHz 70 GHz	Microwave	Power	Microwave (P2P P2MP)	-Spectrum allocation in other bands is required. -Use as is
12	LTE Bands	LTE-M (Cellular)	• Health • Power	3GPP RAN	-Low power RF -Low operating costs Technology under development
13	GSM Bands	NB-GERAN (Cellular)	• Health • Power	3GPP GERAN	-Very low power RF -Very low data rate -Low device & operating costs Technology under development
14	30 GHz to 300 GHz	Millimeter wave (mmWave)	Transport	IEEE 802.11ad	-Line of sight Technology under development

Table 10: Wireless Spectrum and Radio Requirements Analysis

[4] http://www.z-wave.com/

5.2 Wireline Standards

S. No.	Physical Interface	Frequency bands	Verticals	Related Standards	Remarks
1	Serial Interface	Depends on input signal frequency	• Power • Transport	RS-232 RS-422 RS-485	-Use as is
2	Power Line Communication (PLC) 200 Hz – 500 KHz (NB)	<500 KHz	Power	IEEE 1901.2[5]	-Need Regulatory Clarity/Regulations for the use of frequency bands over Power Lines.
		49 KHz – 89 KHz	Power	PRIME	
		35 KHz – 91 KHz	Power	G3-PLC (CENELEC A BAND)	
		98 KHz–122 KHz	Power	G3-PLC (CENELEC B BAND)	
		155 KHz-403 KHz	Power	G3-PLC (ARIB BAND Japan)	
		155 KHz-487 KHz	Power	G3-PLC (ARIB BAND US)	
		10 KHz – 490 KHz	Power	ITU-T G.hnem	
		60 KHz – 76 KHz	Power	IEC 61334	
		200 Hz – 600 Hz	Power	TWACS	
		3 KHz – 148.5KHz	Power	Meters & More	
		10 KHz – 450 KHz	Power	HomePlug C&C	
3	Power Line Communication (PLC) 2 MHz – 30 MHz (BB)	<100 MHz	Power	IEEE 1901-2010	Need Regulatory Clarity/Regulations for the use of frequency bands over Power Lines.
		2 MHz – 30 MHz	Power	HomePlug Green PHY	
		25 MHz – 200 MHz	Power	ITU-T G.hn (G.9960/G9961)	
4	Optical Fiber FTTx	-	• Power • Safety & Surveillance	ITU-T G.651/G.652	-Use as is
5	Ethernet	125 MHz 250 MHz 500 MHz 600 MHz 833.3 MHz 1.2 GHz 1.6 GHz	• Power • Safety & Surveillance	IEEE 802.3	-Use as is
6	USB	-	• Health • Power	USB[6]	-Use as is
7	xDSL	0 MHz – 2.208 MHz	• Power • Transport • Safety & Surveillance	ITU-T G.991, G.992, G.993, G.9700, G.9701	-Use as is
9	OBD-II	-	Transport	SAE standards J1962, J1850	-Use as is

Table 11: Wireline Requirements Analysis

[5] http://standards.ieee.org/findstds/standard/1901.2-2013.html
[6] http://www.usb.org/home

5.3 Network Standards

S. No.	Features	Network Technology	Verticals	Related Standards	Remarks
1	Cellular WAN Packet Network	3GPP	• Power • Health • Safety & Surveillance	GPRS EDGE EPS	-Use as is
		3GPP2	• Health • Safety & Surveillance	1x HRPD	-Use as is
		IEEE	Health	WiMAX (802.16)	-Use as is
2	Short Message	SMS	Health	3GPP TS 23.040/23.041	-Use as is
3	Embedded SIM	eSIM	Transport	GSMA eUICC v2.0 AEC-Q100 ETSI 102671	-Requires regulatory approval.
4	General network stack	IPv6	• Power • Safety & Surveillance	IETF	-Packet flow identification -Fast routing
5		IPv4	• Power • Safety & Surveillance	IETF	-Address space limitation
6	Device network stack (over IEEE 802.15.4 Radio)	6LoWPAN[7]	• Power • Safety & Surveillance	IETF RFC 4919/RFC4944	-Battery drain
		ZigBee IP and 920IP[8]	Power	ZigBee Alliance	-Higher Stack footprint
7	Inter DC Transport	MPLS[9]	Power	IETF MPLS	-Use as is
		L2TP	Power	L2TP (RFC 4951)	-Use as is
8	Network Security	IPsec[10]	Power	IETF IPsec	-Use as is
9	Transport Security	TLS[11]	Power	IETF TLS (RFC 5346/RFC 6347)	-Use as is
10	PAN Security	Bluetooth Security	Health	Bluetooth Security HDPv1.1	-Use as is
11		ZigBee Security	Health	ZigBee HCP	-Use as is
12	Stream Control	RTSP	Safety and Surveillance	IETF RFC 2326	-Use as is
13	Vehicle Diagnostics Network Control	OBD-II	Transport	SAE Standards J2178 series J1939 ISO 14230	-Use as is

[7] https://datatracker.ietf.org/wg/6lowpan/charter/
[8] http://www.zigbee.org/zigbee-for-developers/network-specifications/zigbeeip/
[9] https://datatracker.ietf.org/wg/mpls/charter/
[10] https://datatracker.ietf.org/wg/ipsec/charter/
[11] https://datatracker.ietf.org/wg/tls/charter/

14	Controller Area Network	CAN	Transport	ISO 11898	-Use as is
15	Vehicular Ad-Hoc network (VANET)	Dedicated Short Range Communications (DSRC). Wireless Access in Vehicular Environments (WAVE)	Transport	IEEE 802.11p, IEEE 1609	

Table 12: Network Standards Requirements Analysis

5.4 Service and Information Standards

S. No.	Features	Service Layer Technology	Verticals	Related Standards	Remarks
1	M2M Service Overlay	oneM2M	• Power • Health • Transport • Safety	oneM2M Functional Architecture	-Architecture is scalable and can be used. - Gap analysis and alignment of services and procedures as per regulations is required.
2	Device Management	LWM2M (Wireless)	Health	OMA-DM/L2M2M	-Use as is
3		CPE WAN Management	Health	BBF TR069	-Use as is
4	Entity/Service Authentication	WS-I Basic Security Profile	Health	OASIS WS-I BSP[12]	-Use as is
5	User Identity Management	Aadhaar	• Health • Transport • Safety & Surveillance	UIDAI[13]	-User Identity (Biometric) collection and central storage -Device or Gateway access to User Identity for Authentication
6	XML Encryption	XMLENC	Health	W3C XMLENC[14]	-Use as is
7	Cyber Security & Information Security	ISO/IEC 27000[15]	Power	ISO (27001, 27002)	-Use as is

[12] http://www.ws-i.org/deliverables/workinggroup.aspx?wg=basicsecurity
[13] https://eaadhaar.uidai.gov.in/
[14] http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/Overview.html
[15] http://www.27000.org/

8	Distributed Platform	oneM2M IN	• Health • Safety and Surveillance	oneM2M	-Remote Head end Health Care System to collaborate with Hospital Health Care System. - Interface for distributed interactions for Cloud based platforms are required.
9	Intelligent Transport System	ITS	Transport	ETSI ITS[16] ISO 14813	- Detailed study needs to be conducted.

Table 13: Service and Information Standards Requirements Analysis

5.5 Application Standards

S. No.	Application Feature	Protocols	Verticals	Related Standards	Remarks
1	Smart Meter Data Exchange	DLMS/COSEM [17]	Power	DLMS User Association/IEC 62056	-Use as is
2	Substation Automation	IEC 60870-5-104 and IEC 61850	Power	IEC 60870-5-104 and IEC 61850[18]	-Use as is
3	Electronic Health Record	DOC.MHD 17	Health	BIS MHD 17 HEALTH INFORMATICS SECTIONAL COMMITTEE	-Use as is
4	Electronic Health Communication	ISO 13606	Health	ISO 13606	-Use as is
5	Hospital Workflow	HL7	Health	HL7[19]	-Use as is
6	Health Device Information Exchange	IEEE 11073 Personal Health Data	Health	ISO/IEEE TC 215 11073 series[20]	-Use as is
7	Video Formats	H.264	• Health • Safety & Surveillance	ITU-T H.264	-Use as is
8	Video Camera	ONVIF	Safety &	ONVIF[21]	-Use as is

[16] http://www.etsi.org/technologies-clusters/technologies/intelligent-transport
[17] http://www.dlms.com/index2.php
[18] http://tc57.iec.ch/index-tc57.html
[19] http://www.hl7.org/implement/standards/product_section.cfm?section=1
[20] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=54960
[21] http://www.onvif.org/

	Communication		Surveillance		
9	Vehicle Diagnostics	OBD	Transport	SAE OBD Standards J1978, J1979, J2012 ISO 15765	-Use as is
10	Vehicle Emission Information exchange	ISO 15031	Transport	ISO 15031	-Use as is

Table 14: Device to Gateway Application Requirements Analysis

6. Way Forward

6.1 General

It is now important for all the verticals to study the Service Delivery Models described in this document and try to do a gap analysis with their existing deployments. Proper estimation of the growth of users in each Industry segment and all combined would be necessary to fine tune the architecture. Need for interworking proxy for different vertical centric applications shall be identified so that the common service layer can be seamlessly adopted across industries. A common M2M service layer provides economies of scale for delivering M2M application and services across all verticals. Since most elaborate and exhaustive work has been done by oneM2M to define a generic architecture which leverages on Common Service Layer, it would therefore be most appropriate to consider oneM2M architecture as the standard architecture by the verticals. The various verticals/industry segments are expected to analyze the oneM2M architecture with respect to their applications and suggest tailoring, if required.

It is also important for the vertical industries provide details of their applications like payload size, acceptable latency figures, expected volume of M2M application users etc. so that the network and M2M service providers can do the sizing and design the infrastructure to cater to the requirements of the entire M2M ecosystem.

6.2 Key Recommendations

6.2.1 Adoption of oneM2M Architecture as base

While many applications were in place for industry segments following a 'Vertical Architecture', it was considered necessary to adopt an open standard based 'Horizontal Architecture.

Since lot of progress towards framing the architecture has been made by OneM2M, the same may be adopted as the base architecture and India specific tailoring be done on that (if needed by any specific use case for any vertical).

6.2.2 Naming and Addressing

It would then become necessary to have a common addressing scheme which would allow all M2M devices to have unique name and address. A detailed study and analysis of M2M Naming & Addressing methodology would have to be done to come out with a comprehensive scheme.

6.2.3 Network

In view of the future requirements where it would be necessary to uniquely address each device, it was considered to be most appropriate to consider IPv6 as the protocol of choice and is therefore recommended at the Device/Gateway level and beyond. Till its maturity, dual stack may be permitted.

Keeping in view the huge volume of devices in M2M, IPv6 (or Dual Stack i.e. IPv4 and IPv6) may be adopted as a standard. The possible use case scenarios and deployment challenges have to be studied further.

6.2.4 Security

Security is one of the most important considerations while designing an M2M system, in order to prevent the hackers to break into M2M applications designed to control, for example, building security, environmental monitoring, vehicle tracking, etc. In order to prevent possible security violations, the most appropriate communication techniques must be used, because different types of communication techniques present different encryption and security features. The oneM2M architecture defines the security framework for building more intelligent and autonomous M2M system. It attempts to resolve the security issues in communication and control problems between machines with difference in technical characteristics that make them part of the global Internet network. The secure software framework allows systems to function in different application domain. Providing reliable services is complicated by the fact that different parts of the network are provided by different entities

The security analysis of the general M2M Network Architecture and the deployment models considering oneM2M security framework has to be further studied in detail.

6.2.5 Spectrum

Effective use of the available Spectrum by using innovative methods would be an important area of study and development as the communicating devices would be huge in numbers. In addition to that Sub GHz, TVWS, mmWave spectrums may be further investigated for allocation and assignment to M2M applications. The health aspects would also have to be kept in mind while studying and developing solutions utilizing these frequencies.

6.2.6 Make in India

To boost manufacturing in India and avoid grey market products proliferate in the market, TEC Type approval and interface approval may be considered for M2M devices and APIs

7. References

1. The Internet of Things – How the Next Evolution of the Internet is Changing Everything, Link (Available on 1st Feb'15): http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
2. Fielding, Roy Thomas (2000). "Chapter 5: Representational State Transfer (REST)". Architectural Styles and the Design of Network-based Software Architectures (Ph.D.). University of California, Irvine. Link (Available on 1st Feb'15): http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm
3. Hypermedia as the Engine of Application State (HATEOAS), Link (Available on 1st Feb'15): http://en.wikipedia.org/wiki/HATEOAS
4. oneM2M Functional Architecture Release 1.0, Link (Available on 1st Feb'15): http://www.onem2m.org/images/files/deliverables/TS-0001-Functional_Architecture-V1_6_1.pdf
5. Architecture Analysis - Part 1: Analysis of architectures proposed for consideration by oneM2M, Link (Available on 1st Feb'15): http://www.onem2m.org/images/files/deliverables/oneM2M-TR-0002-Architecture_Analysis_Part_1-V0_2_0.doc
6. Architecture Analysis - Part 2: Study for the merging of architectures proposed for consideration by oneM2M, Link (Available on 1st Feb'15): http://www.onem2m.org/images/files/deliverables/oneM2M-TR-0003-Architecture_Analysis_Part_2-V0_5_0.doc
7. M2M Communications in the Indian Power Sector, 6th Apr'15, TEC M2M Power Vertical WG, File: DoT - M2M Roadmap Power Sector Final - April 6.docx
8. M2M Health - Working Group, Revision number – 0.2.1, 30th Mar'15, TEC M2M Health Vertical WG, File: M2M_Health_WorkingDocument_v0.2.1.docx
9. M2M Communications in the Safety and Surveillance, TEC M2M Safety and Surveillance Vertical WG, File: DoT-M2M Roadmap Safety and Surveillance_V6.docx
10. Intelligent transport system – India, TEC M2M Transport Vertical WG, File: M2M WG TR#1 -ITS M2M v17 (2).docx
11. G. Lawton, "Machine-to-Machine Technology Gears Up for Growth", Computer, vol. 37, (2004)

ISO 9001:2008

TELECOMMUNICATION ENGINEERING CENTRE
DEPARTMENT OF TELECOMMUNICATIONS
MINISTRY OF COMMUNICATIONS & INFORMATION TECHNOLOGY
GOVERNMENT OF INDIA