International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series Y

Supplement 53

(12/2018)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

ITU-T Y.4000-series – Internet of Things use cases

ITU-T Y-series Recommendations – Supplement 53

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Supplement 53 to ITU-T Y-series Recommendations

ITU-T Y.4000-series – Internet of Things use cases

Summary

Supplement 53 to ITU-T Y-series Recommendations provides use cases related to different application domains of the Internet of Things.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y Suppl. 53	2018-12-13	20	11.1002/1000/13867

Keywords

Internet of Things, IoT, use case.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g.,, interoperability or applicability) and compliance with the publication is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at .

Table of Contents

Supplement 53 to ITU-T Y.4000 series

ITU-T Y.4000-series – Internet of Things use cases

1 Scope

This Supplement provides use cases related to different application domains of the Internet of things (IoT). Specifically, this Supplement covers:

– Part 1 – Recommended template for the description of IoT use cases (clause 6);

– Part 2 – Classification scheme for IoT use cases (clause 7);

– Part 3 – A set of IoT use cases (collected by Q2/20 from inputs of the ITU-T membership) (clause 8).

NOTE 1 – The use cases are not intended to be prescriptive or promote specific technologies or solutions.

NOTE 2 – This Supplement has adopted a classification scheme for internal classification purposes only.

2 References

[ITU-T E.161.1] Recommendation ITU-T E.161.1 (2008), *Guidelines to select Emergency Number for public telecommunications networks*.

[ITU-T HSTP-H810] ITU-T Publication (2017), *Fundamentals of data exchange within ITU-T H.810 Continua Design Guideline architecture*. <http://handle.itu.int/11.1002/pub/80f6d9f9-en>

[ETSI TS 102 225] ETSI TS 102 225 V12.1.0 (2014-10), *Smart Cards; Secured packet structure for UICC based applications (Release 12)*.

[ETSI TS 102 267] ETSI TS 102 267 V11.0.0 (2012-12), *Smart Cards; Connection Oriented Service API for the Java CardTM platform (Release 7)*.

[ETSI TS 102 671] ETSI TS 102 671 V9.2.0 (2015-06), *Smart Cards; Machine to Machine UICC; Physical and logical characteristics (Release 9)*.

[ETSI Smartcards] ETSI Website, *Smart Cards*. <https://www.etsi.org/technologies/smart-cards>

[ETSI SIM] ETSI Website, *SIM*. <https://www.etsi.org/technologies/smart-cards/sim>

[IEEE-ESD] IEEE, *Improved output ESD protection by dynamic gate floating design*. <https://ieeexplore.ieee.org/abstract/document/711378>

[4G-America] 4G Americas (2015), *Cellular technologies enabling IoT*. <http://www.5gamericas.org/files/6014/4683/4670/4G_Americas_Cellular_Technologies_Enabling_the_IoT_White_Paper_-_November_2015.pdf>

[ARA-India] The Automotive Research Association of India, *Intelligent Transportation Systems (ITS) – Requirements for Public Transport Vehicle Operation*. <https://araiindia.com/hmr/Control/AIS/921201744153PMAIS-140.pdf>

[AlMR] Allied Market Research, *Remote Patient Monitoring Market by Condition (Congestive Heart Failure, Diabetes, Chronic Obstructive Pulmonary Disease, Blood Pressure, and Mental Health), Components (Devices and Software) – Global Opportunity Analysis and Industry Forecast, 2014 – 2022*. <https://www.alliedmarketresearch.com/remote-patient-monitoring-market>

[BIS-India] Bureau of Indian Standards, *Core Activities*. <http://www.bis.org.in/sf/ted/TED28(10974)_24112016.pdf>

[CDSCO] UIndian Pharmacopoeia Commission, National Coordination Centre-Materiovigilance Programme of India Ministry of Health & Family Welfare, Government of India, *A GUIDANCE DOCUMENT for MEDICAL DEVICE*. <http://www.cdsco.nic.in/writereaddata/Guidance Document ipv.pdf>

[Commonwealth Fund] The Commonwealth Fund, *Medicaid's Future: What Might ACA Repeal Mean?* <http://www.commonwealthfund.org/publications/issue-briefs/2017/jan/medicaids-future-aca-repeal>

[DoT-India] Government of India, Ministry of Communications, Department of Telecommunications, *All CMTS/UAS/UL (having Access Services Authorization) Licensee(s).* <http://www.dot.gov.in/sites/default/files/M2M Guidelines.PDF?download=1>

[FDA-Transparency] U.S. Food and Drug Administration, *What does FDA do?* <https://www.fda.gov/AboutFDA/Transparency/Basics/ucm194877.htm>

[Forbes] Forbes, *All Cars In Europe Can Now Call The Police Themselves*. <https://www.forbes.com/sites/davekeating/2018/04/01/starting-today-all-cars-in-europe-can-call-the-police-themselves/>

[Gartner] Gartner Website. <https://www.gartner.com/newsroom/id/3204017>

[GSMA-mAuto] GSMA Connected Living programme: mAutomotive (2012), *2025 Every Car Connected: Forecasting the Growth and Opportunity*. <http://www.gsma.com/connectedliving/wp-content/uploads/2012/03/gsma2025everycarconnected.pdf>

[GSMA-SIM] GSMA Website, *SIM Working Group, Embedded SIM*. <https://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/sim-working-group/embedded-sim>

[Health Affairs] Health Affairs, *CBO Lowers Marketplace Enrollment Projections, Increases Medicaid Growth Projections*. <http://healthaffairs.org/blog/2016/01/26/cbo-lowers-marketplace-enrollment-projections-increases-medicaid-growth-projections/>

[IAB IPV6] Internet Architecture Board, *IAB statement on IPv6*. <https://datatracker.ietf.org/liaison/1545/>

[Indian Express] The Indian Express, *Road accidents in India, 2016: 17 deaths on roads every hour, Chennai and Delhi most dangerous*. <http://indianexpress.com/article/india/road-accidents-in-india-2016-17-deaths-on-roads-every-hour-chennai-and-delhi-most-dangerous-4837832/>

[Indian Infra Pub] India Infrastructure Publishing Website, *Smart Meter Rollout*. <https://powerline.net.in/2018/02/09/smart-meter-roll/>

[JAMA] The Journal of the American Medical Association, *The Medicare Hospital Readmissions Reduction Program: Time for Reform*. <https://www.wicker.senate.gov/public/_cache/files/5880d2d4-a727-4ee9-9def-7991058e4584/jama-the-medicare-hospital-readmissions-reduction-program.pdf>

[MarketsandMarkets] MarketsandMarkets Website, *Home Automation System Market by Protocol and Technology (Network and Wireless), Product (Lighting, Security and Access Control, HVAC and Entertainment Control), Software and Algorithm (Behavioral and Proactive), and Geography – Global Forecast to 2022*. <https://marketsandmarkets.com/Market-Reports/home-automation-control-systems-market-469.html>

[microservices.io] microservices.io Wbesite, *Pattern: Microservice Architecture*. <https://microservices.io/patterns/microservices.html>

[Nash 2016] Nash II, Don, Mwakalonge, Judith, and A. Perkins, (2016). *An investigation of factors influencing performance of Radio Frequency Identification (RFID): applications in transportation*. Journal of Transport Literature, pg. 25-29.

[NITI Aayog-A] National Institution for Transforming India, Government of India, *Maternal Mortality Ratio (MMR) (per 100000 live births)*. <http://niti.gov.in/content/maternal-mortality-ratio-mmr-100000-live-births>

[NITI Aayog-B] National Institution for Transforming India, Government of India, *Infant Mortality Rate (IMR) (per 1000 live births)*. <http://niti.gov.in/content/infant-mortality-rate-imr-1000-live-births>

[OASIS] OASIS (2015), *MQTT Version 3.1.1 Plus Errata 01- OASIS Standard Incorporating Approved Errata 01*. <http://www.opengroup.org/soa/source-book/soa_refarch/p18.htm>

[oneM2M TS 0002] OneM2M TS 102 267 V7.1.0 (2010-04), *OneM2M Technical Specifications – Requirements*. <http://www.onem2m.org/images/files/deliverables/TS-0002-Requirements-V1_0_1.pdf>

[oneM2M Drafts] OneM2M Website, *Standards for M2M and the Internet of Things*. <http://www.onem2m.org/technical/published-drafts>

[Open Group] The Open Group, *SOA Reference Architecture – Relationship to Other SOA Standards)*. <http://www.opengroup.org/soa/source-book/soa_refarch/p18.htm>

[Sim Alliance] Sim alliance, *eUICC for: Connected cars*. <http://simalliance.org/wp-content/uploads/2017/10/eUICC-for-Connected-cars_FINAL.pdf>

[Society-5.0] Cabinet Office, Government of Japan, *Society 5.0*. <http://www.who.int/ageing/publications/global_health.pdf>

[TEC-India-M2M] Telecommunication Engineering Center, Ministry of Communications, Department of Telecommunications, Government of India, *Technical Report on M2M Enablement in Remote Health Management*. <http://tec.gov.in/pdf/M2M/M2M Enablement in Remote Health Management.pdf>

[TEC-MTCTE] Telecommunications Engineering Centre, Ministry of Communications, Department of Telecommunications, Government of India, *Mandatory Testing and Certification of Telecom Equipments (MTCTE)*. <http://www.tec.gov.in/mandatory-testing-and-certification-of-telecom-equipments-mtcte/>

[TEC Reports] Telecommunication Engineering Center, Ministry of Communications, Department of Telecommunications, Government of India, *Technical Report on M2M Enablement in Remote Health Management*. <http://www.tec.gov.in/technical-reports/>

[TRAI] Telecom Regulatory Authority of India (2017), *Recommendations on Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications*. <https://trai.gov.in/sites/default/files/Recommendations_M2M_05092017.pdf>

[UN-MDG] United Nations, *Millennium Development Goals (MDG)*.

[WHO-GHA] World Health Organization, *Global Health and Aging*. <http://www.who.int/ageing/publications/global_health.pdf>

[WHO-ICD] World Health Organization, *International Statistical Classification of Diseases and Related Health Problems*. 10th Revision, Volume 2 Instruction manual, 2010 Edition. <http://www.who.int/classifications/icd/ICD10Volume2_en_2010.pdf>

[WHO-India] World Health Organization, *Countries, India*.

<http://www.who.int/countries/ind/en/>

[World-Bank-A] The World Bank, *Rural population (% of total population)*. <https://data.worldbank.org/indicator/SP.RUR.TOTL.ZS>

[World-Bank-B] The World Bank, *Physicians (per 1,000 people)*. <https://data.worldbank.org/indicator/SH.MED.PHYS.ZS>

[YaleNews] YaleNews, Yale University, *Six strategies for reducing hospital readmissions among elderly*. <http://news.yale.edu/2013/07/16/six-strategies-reducing-hospital-readmissions-among-elderly>

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Supplement

None.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

AHD Application Hosting Device

AMI Advanced Metering Infrastructure

API Application Program Interface

BPL Below the Poverty Line

BT Bluetooth

BTLE Bluetooth Low Energy

CAGR Compounded Annual Growth Rate

CAN Car Area Network

CDMA Code Division Multiple Access

DLMS Device Language Message Specifications

DSRC Dedicated Short-Range Communication

ECG Electrocardiography

EC-GSM Extended Coverage – GSM

EHR Electronic Health Record

e-KYC electronic Know Your Customer

EMC Electromagnetic Compatibility

EMI Electromagnetic Interference

EMR Electronic Medical Records

e-SIM embedded Subscriber Identity Module

ERP Enterprise Resource Planning

eUICC Embedded Universal Integrated Circuit Card

FCC	Federal Communications Commission
FDA	Food and Drug Administration
FOTA	Firmware Over-the-Air
GIS	Geographical Information System
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile communication
GSMA	GSM Association
HAN	Home Area Network
HES	Head-end System
HIE	Health Information Exchange
HRN	Health Record Network
HT, LT	High Tension, Low Tension
IccID	Integrated circuit card Identifier
IHD	In-home Display
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IMEI	International Mobile Equipment Identity
IoT	Internet of Things
ISM	Industrial, Scientific and Medical
ISO	International Organization for Standardization
ITS	Intelligent Transport System
KYC	Know Your Customer
LAN	Local Area Network
LTE	Long Term Evolution
LPWAN	Low-Power Wide Area Network
LoRa	Long-Range applications
M2M	Machine to Machine
M2MSP	M2M Service Provider
MBC	Metering, Billing, Collection
MDMS	Meter Data Management System
NAN	Neighbourhood Area Network
NB-IoT	Narrowband Internet of Things
NFC	Near-field Communication
NiBP	Noninvasive Blood Pressure
OBD	On-board Diagnostics
OMS	Outage Management System

OTA	Over the Air
PAN	Personal Area Network
PCH	Personal Connected Health
PERS	Personal Emergency Response System
PHI	Protected Health Information
PLCC	Power Line Carrier Communication
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
QoS	Quality of Service
REST	Representational State Transfer
RFID	Radio Frequency Identification
RPM	Remote Patient Monitoring
SAR	Specific Absorption Rate
SIM	Subscriber Identification Module
SMS	Short Message Service
Sub-Gig	Sub Giga Hz Radio Communication
TAN	Touch Area Network
TSP	Telecom Service provider
USB	Universal Serial Bus
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
VSAT	Very Small Aperture Terminal
WAN	Wide Area Network
WiFi	Wireless Fidelity

5 Conventions

None.

6 Part 1 – Recommended template for the description of IoT use cases

Recommended template

1. Title of the use case (title is strictly related with the application area addressed)
    a. Name of the use case
    b. ID of the use case (ID will be given by ITU-T SG-20 such as vertical name/001/16-17)
    c. Version/revision history (such as no./month/year)
    d. Source (country/ITU-T member/organization registered with ITU)
2. Objective of the use case (aligned with title, it has explanatory content)
3. Background

a. Current practice (current process/context which will benefit from the implementation of the use case)
b. Need for use case
c. Country ecosystem specifics

4. Description
   a. Ecosystem description in terms of actors and business roles
   b. Contextual illustration
   c. Prerequisites
   d. Preconditions (if any)
   e. Triggers
   f. Scenario

   NOTE – The option to have a single scenario per single use case is the basic one. However, multiple scenarios for a single use case are not prevented; in this case, they are indicated in this same field as appropriate.

   g. Process flow diagram
   h. Post-conditions (if any)
   i. Information exchange

   NOTE – It is expected to have the information exchange (field i) associated with the process flow (and process flow diagram if any) (field g).

5. Architectural considerations
   a. Deployment considerations
   b. Geographical considerations
   c. Communication infrastructure
   d. Performance criteria
   e. Interface requirements
   f. User interface
   g. Application program interfaces (APIs) to be exposed to the application from platform
   h. Data management
   i. Data backup, archiving and recovery
   j. Remote device management
   k. Startup/Shutdown process
   l. Security requirements
6. Potential market growth forecast
7. Implementation constraints (for the support of the use case)
8. Statutory compliances and related regulations
9. Available international standards
11. General remarks

7 Part 2 – Classification scheme for the IoT use cases

Classification

The ID of each use case is composed by the combination of:

– Name of the (IoT-enabled) vertical domain;

– Sequential number of the use case in the related vertical domain.

Examples of vertical domains are provided in the Table 7-1.

Table 7-1 – IoT vertical do main examples

Vertical domain number	Vertical domain	Vertical related applications
1	Automotive/ Intelligent transport system (ITS)	Vehicle tracking, eCall, vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) applications, traffic control, navigation, infotainment, fleet management, asset tracking, manufacturing and logistics
2	Utilities / Energy	Smart metering, smart grid, electric line monitoring, gas/oil/water pipeline monitoring
3	Healthcare	Remote monitoring of patient after surgery (e-health), remote diagnostics, medication reminders, telemedicine, wearable health devices
4	Safety	Commercial and home monitoring, surveillance camera applications, video analytics and sending alerts, fire alarm, police/medical alert
5	Financial	Point of sale (POS), ATM, digital signage and handheld terminals
6	Retail	Kiosk, vending machines, retail stores
7	Smart city	ITS, waste management, street-light control system, water distribution, smart parking, intelligent buildings, safety
8	Smart home	Home alarm systems, connected appliances, smart lighting system, home entertainment
9	Agriculture	Remotely controlled irrigation pump, crop management, soil analysis, livestock monitoring
10	Smart manufacturing	Proactive maintenance of machines, shop-floor monitoring, industry automation
11	Supply chain management	Demand assessment, inventory management, cargo tracking, retail management, customer feedback, connected supply chain
12	Smart water management	Smart metering

8 Part 3 – IoT use cases

This clause reports information collected by ITU-T Study Group 20 from its membership.

8.1 Remote monitoring of health of a patient

1. Title of the use case
   a. Name of the use case: Remote monitoring of the health of a patient
   b. ID of the use case: Health/001/2017
   c. Version/revision history: 1.5/Dec/2018
   d. Source: India/MoC/TEC
2. Objective of the use case

   This use case describes the building blocks for remote patient monitoring (RPM) – that would enable key health data from the patient or the user to be uploaded to an electronic health record (EHR) system monitored by the health care service provider.

This, in turn, allows the healthcare service provider to have access to current health data of the patient and be able to plan care services for the patient remotely. Thus, a doctor would be able to review the health condition of the patient remotely, without the patient having to travel to meet the doctor.

3. Background

a. Countries specific health scenario

The World Health Organization (WHO) provides health challenges and demographic information on its website for the member countries.

The Global Health Observatory (GHO) "by country" view provides a set of summary statistics for each member state. These statistics provide a high-level overview of a country's health indicators.

Specific information for India is available at [WHO-India].

The following use case is generic in nature and may be applicable to all countries.

b. Current practice

The existing infrastructure for telemedicine or RPM is inadequate in numerous countries and regions of the world to address the growing healthcare needs. There are a few instances in numerous countries and regions of the world where technology is used for example, teleconsultation between a city-based tertiary hospital and a satellite healthcare centre in a smaller town.

However, in some countries and regions of the world with inadequate telemedicine/RPM infrastructure, some hospital chains have pioneered telemedicine using very small aperture terminal (VSAT) leased lines, cellular technologies and have provided access to secondary/tertiary consulting services to remote rural healthcare centres. Most of the tele-consultations were reviews of medical cases. However, this facility is not available in many countries and regions, and may be expensive to maintain. Full-fledged RPM initiatives are still lacking wide adoption and have not been taken up even in metropolitan and urban areas.

c. Need for use case

The key factors that impact healthcare are:

Problems specific to countries with a poor population:

For example, India which poses a unique set of challenges when it comes to "accessibility of quality healthcare"

Problems specific to countries where a significant percentage of the population is below the poverty line (BPL).

- India is one of the most populous countries, with more than 66% of its population in rural areas [World-Bank-A] and around 21% BPL [UN-MDG].
- Doctors are not available in adequate numbers [World-Bank-B].
- Where physical infrastructure is available, trained human resources are limited.
- The low level of education and financial strength in this impoverished group, leads to a lower ability to purchase and use technology solutions.
- Poor health report card: Maternal mortality ratio (MMR) (per 100000 live births: MMR for India is 130 for 2014-16 [NITI Aayog-A] and Infant Mortality Rate (IMR) (per 1000 live births: For India was 34 for 2016 [NITI Aayog-B] are often high. Highest burdens of communicable diseases and lifestyle changes often lead to a spurt in non-communicable diseases (e.g., diabetes and hypertension).

General problems across various countries:

- Skewed healthcare infrastructure with most of the infrastructure concentrated in urban areas.
- The number of beds and number of doctors per 1000 people is low. As a result, doctors are overworked leading to inadequate medical treatment and/or very long waiting times.
- A well-planned RPM framework built on top of a robust infrastructure would ease the burden on the present healthcare system in developing countries and at the same time provide access to quality healthcare that is affordable.

d. Ecosystem specifics

Some of the key challenges seen in RPM systems in developing countries are as follows:

- Lack of supportive infrastructure to roll out RPM services.
- Lack of or limited established and approved standards as well as clinical protocols for delivering remote healthcare services.
- Lack of established and approved standards for healthcare device safety and usage.
- High cost of subscribing for individual RPM devices and subscription services as it is primarily borne by the patient.
- Availability of affordable healthcare devices.
- A biased perception towards healthcare devices, as patients would prefer to see a doctor than rely on a healthcare device.
- Lack of patient education in remote health care.
- Lack of comfort within medical fraternity in moving from traditional medical practices to adopting new technologies.
- Availability of human resource trained in using a new technology.

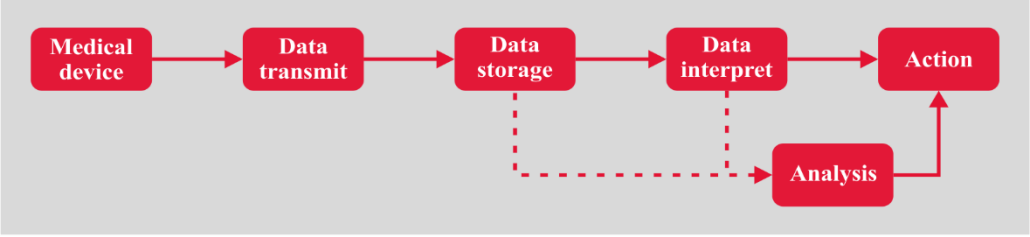
4. Description

a. Ecosystem description in terms of actors and business roles

RPM is a mobile or telehealth solution that enables monitoring of patients outside of conventional clinical settings (e.g., in the home). The patient has the healthcare device on or close to their body which has sensors that capture the patient's healthcare/ physiological data. This data is then transferred across telecommunications networks with the help of data transmission products, and is monitored for specific predefined parameters with the help of software and/or clinical and healthcare experts.

Increasing number of people with chronic medical conditions and growing senior citizen population, coupled with shortages of skilled medical personnel have been driving the demand for remote health services all over the world. By increasing reach and efficiency of doctors, RPM helps increase access to care and will eventually decrease healthcare delivery costs.

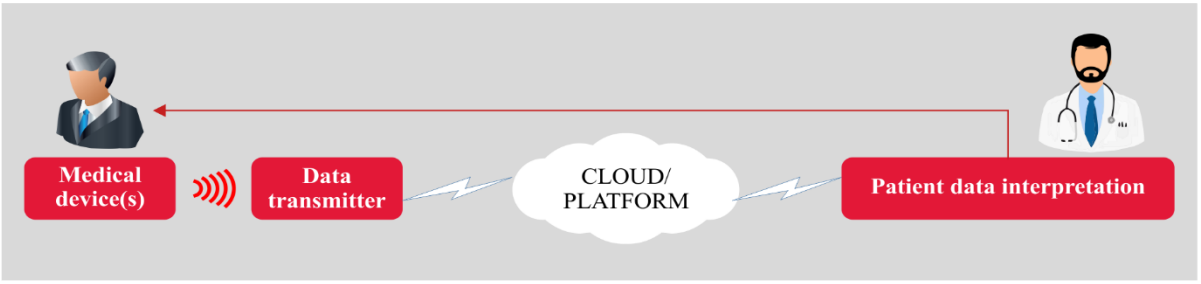
It addresses a key pain point of the stakeholders of the healthcare system by enabling the exchange and flow of information from a patient's healthcare device (outside of hospital) to the clinical staff such as doctors, nurses and paramedics.



NOTE 1 – See [TEC-India-M2M]
NOTE 2 – Source [GSMA-mAuto]

Figure 8-1 – Information flow in remote patient monitoring

RPM helps in monitoring patients' medical conditions, makes available early diagnosis and even reduces or prevents medical emergencies and hospital readmissions. It also helps those in geographically isolated settings to access specialized and preventive medicine and care.



NOTE – Source [GSMA-mAuto]

Figure 8-2 – Remote patient monitoring concept

Components of RPM solution:

- Sensors on a device that is enabled by wired or wireless communications to measure physiological parameters.
- Local data storage at patients' site that interfaces between the devices and other centralized data repository and/or healthcare providers.
- Data transmission and connectivity.
- Centralized repository to store data.
- Diagnostic application software that develops treatment recommendations and intervention alerts based on the analysis of collected data. This may be augmented by medical experts such as doctors, nurses.
- Depending on the disease and the parameters that are monitored, different combinations of sensors, storage and applications may be deployed.
- Depending on the criticality of the data and the regulations around it being gathered, personal devices can be categorized into a few classes. The followings are three classes identified by the US Food and Drug Administration (FDA); see [ETSI TS 102 671]:

  i. Class I devices are deemed to be low-risk devices and are therefore subject to the least regulatory controls. For example, dental floss, elastic bandages, handheld dental instruments and examination gloves have been classified as Class I device.

ii. Class II devices are higher risk devices than Class I and require greater regulatory controls to provide reasonable assurance of the device's safety and effectiveness. For example, X-ray machines, powered wheelchairs, infusion pumps, surgical and acupuncture needles are classified as Class II devices.

iii. Class III devices are generally the highest risk devices and are therefore subject to the highest level of regulatory control. Class III devices must typically be approved by FDA before they are marketed. For example, implanted pacemakers, replacement heart valves are classified as Class III devices.

See [FDA-Transparency] and [CDSCO].

b. Contextual illustration

Contextual illustration actor descriptions are provided in Table 8-1.

Table 8-1 – Actor description

Actor name	Actor type (person, organization, device, system)	Role description
Patient	Person	The person whose parameters are to be monitored. The monitoring could be in a clinical or non-clinical setting.
Personal device/health care device	Device	Interfaces on one side with the physical world, measures patient's vitals (e.g., noninvasive blood pressure (NiBP), blood sugar, electrocardiography (ECG), weight). Interfaces with a medical gateway at the other side. This interface could be either wired (universal serial bus (USB)) or wireless (e.g., Bluetooth (BT), Bluetooth low energy (BTLE), ZigBee) and these devices may either be single or multi parameter monitors. These devices may use proprietary protocol to communicate with the gateway or use a standard protocol like International Organization for Standardization (ISO)/Institute of Electrical and Electronics Engineers (IEEE) 11073.
Medical gateway	Device	The device that interfaces with the personal devices at the patient's location, aggregates the information and communicates with the backend system (EHR/PHR/CIS). This gateway could be a dedicated hardware-based device, or software on a personal computer, laptop or smart phone.
Communication infrastructure (backbone)	System	This infrastructure forms the back bone of the RPM setup. It could be a combination of land-line/mobile telecom infrastructure providing internet connectivity.
Medical records	System	The database at the backend (could be a hospital-based electronic medical records (EMR), a public PHR or any type of clinical information system.
RPM application platform	System	This could be an application framework that leverages the medical records information and provides the care provider a customized interface

Table 8-1 – Actor description

Actor name	Actor type (person, organization, device, system)	Role description
		depending on the end-application (e.g., chronic disease management, clinical trials).
Tele healthcare Provider	Organization/person	It includes doctors, nurses and other telehealth staff (can be paramedics) who are involved in monitoring the vitals and evaluating the information.
Clinician/doctor		It includes doctors/clinicians who can intervene based on data and feedback from telehealth care providers, to take appropriate action for the patient.

c. Prerequisites (Assumptions)

It is assumed that:

- Patients or their caregivers are capable of using personal devices.
- Doctors are willing and capable of interpreting medical data and using EHRs as part of the diagnostic and treatment process.
- Formal training is required for persons managing RPM to make it more effective.
- Local considerations should be taken into account for both patients and healthcare providers.
- All EHRs in which the parameters remotely monitored are documented must have the following sections:
  i. Relevant past clinical history
  ii. Present clinical problems

Ideally, unless these two columns are populated, an entry should not be allowed to be made for any parameter in which health is being monitored.

d. Preconditions (if any)

It is assumed that:

- The personal health monitoring device is being worn/used by the user appropriately to make accurate data measurement.
- The communication between personal device and aggregator (medical gateway) is working and the user is able to identify the communication channel availability.
- The wide area network (WAN) connectivity is available from aggregator to the EHR system.
- The user has agreed by contract to subscribe to the health parameter monitoring and records update:
  i. When a "personal" device is being used, the user identity is managed by the unique-ID of the personal device which is either updated in the cloud application or by assigning device ID to the specific user. In case a shared device is used, there needs to be another mechanism to identify the user of the device uniquely.
  ii. Related regulations for these activities are in place.

e. Triggers (if any)

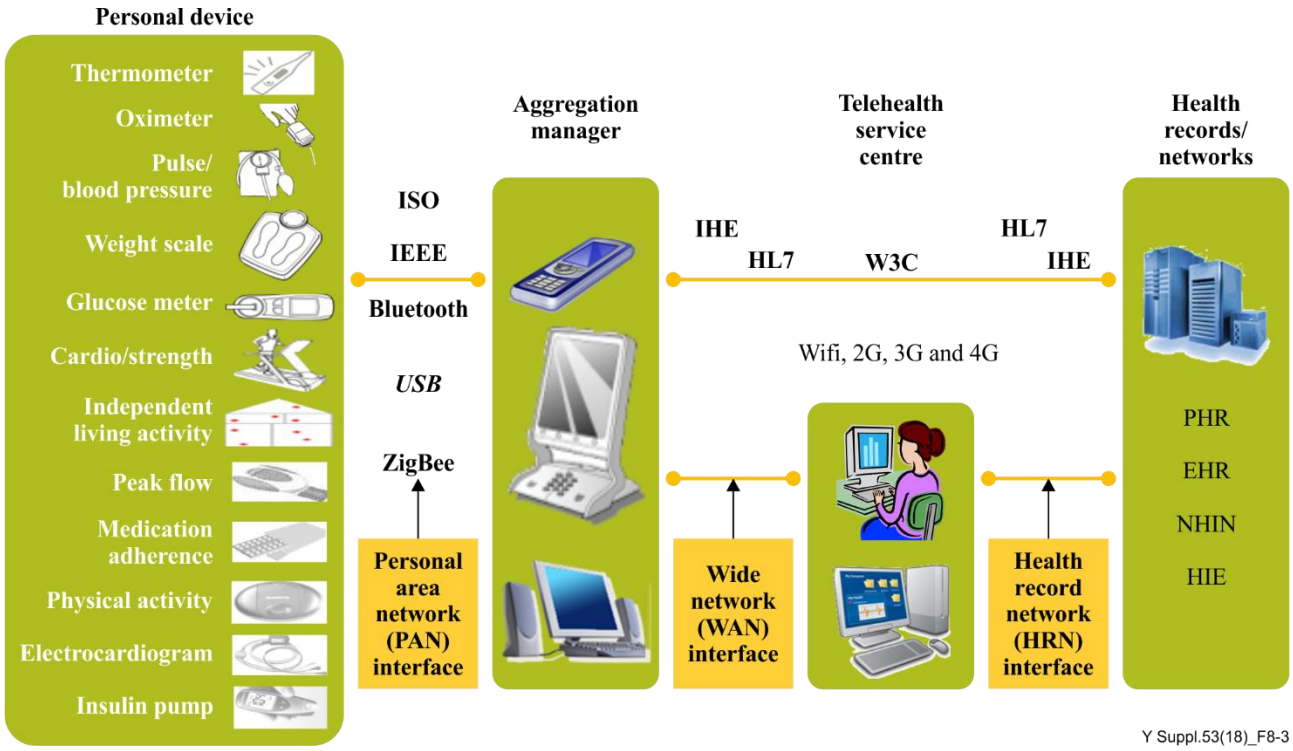
- When a personal device is being used, this will trigger the use case for collecting the data and sending it to the servers.
- An action from a doctor will be triggered when data received from the patient is abnormal/deranged.

f. Scenario

- The personal health monitoring device is worn/used by a user to make appropriate data measurement.
- The device or an external mechanism is able to identify the user, whose data is being captured, in a unique manner.
- The initial pairing of the personal device and the medical gateway/aggregator device can be done during the system installation and configuration, or on the fly, in case of a mobile patient.
- Once the measurement is made on the personal device, this data is transferred to the gateway device over a local communication protocol such as Bluetooth, near-field communication (NFC), ZigBee, etc.
- The data is then transferred from the medical gateway to a central server holding the patient's EHR over a fixed or wireless network in a private and secure fashion, using WAN protocols.
- Once the EHR has been updated, medical protocols / guidelines may be applied either by the system or telehealth support personnel or nurses or clinicians, on the data.
- This may initiate health alerts, when the data is found to be out of range.
- Doctors or clinicians may take appropriate actions as per-care pathways based on the data and/or health alerts. Actions may vary from emergency care to a general health advice.

g. Process flow diagram

- The detailed analysis can lead to a variety of actions, for example, long-term recommendations for an individual or disease analysis for a population, which may lead to further intervention planning, both at the individual patient level or policy level.



NOTE – Source [4G-America]

Figure 8-3 – Remote health monitoring architecture by Continua Health Alliance

h. Post-conditions

- The data is stored in the EHR system with a timestamp.
- The data can be further analysed at the cloud services database.
- Data analysis should not only be confined to monitor parameters but should also specifically include nature of intervention (Nil/OP/IP/surgery). Clinical diagnosis as per ICD 10 [WHO-ICD] should be made mandatory in every EHR.

i. Information exchange

Data bandwidth requirements

- Data bandwidth requirements are dependent on the personal device of patient being monitored and the frequency of data transfer.
- Based on the range of devices available/put to use, the data bandwidth requirements differ.
- Sometimes, the remote device or gateway device may store the data and all data is forwarded in bulk when network connectivity is available.

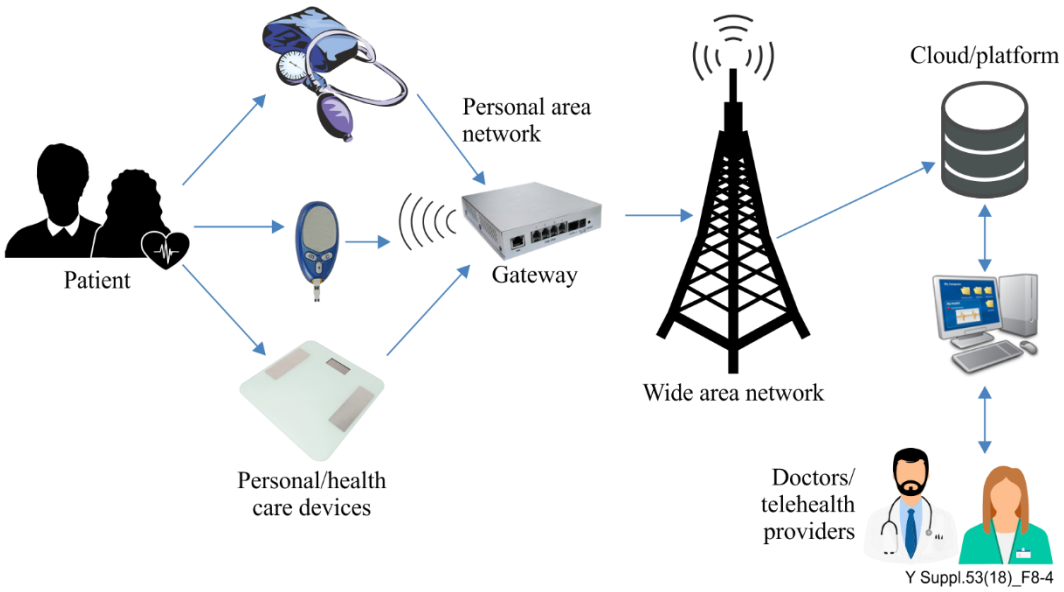
5. Architectural considerations (non-functional requirements)

a. Deployment considerations

A personal health monitoring device can be worn by a person or be placed near the person's body.

The environments which can implement health monitoring services include, but are not limited to, personal home, health care institution, hospital, ambulance.

A personal health monitoring device can be static or mobile, and a diversity of communication network technologies (e.g., Bluetooth, USB, cellular technologies) are needed to support health monitoring services.



NOTE – Source [TEC-India-M2M]

Figure 8-4 – Pictorial view of communication infrastructure

Communication channel used:

- Wired communication like serial port, USB and audio port, etc.
- Wireless data transmission channels such as Bluetooth, wireless fidelity (WiFi) and telecom connectivity.

b. Geographical consideration (for geographical spread and concentration of the constituent devices)

The healthcare devices are personal devices, which shall not affect any limitations or challenges for the geographical spread. Actually, each single user can have several healthcare devices.

The WAN connectivity is assumed to be available and enough to carry the data from all users in case of concentration of the devices.

In addition, the data packets in health devices are small and transmissions are sporadic in nature. No specific challenge for the geographical consideration is expected.

In case of rural healthcare, the same considerations apply.

c. Communication infrastructure

Communication technologies in personal area networks (PANs) and WANs are given in Table 8-2:

Table 8-2 – Communication technologies

Scenario	Communication network	Technologies
Devices to be connected directly to the head-end system	WAN	Global system for mobile communication (GSM) 2G, 3G, long term evolution (LTE); WiFi, code division multiple access (CDMA), fixed line broadband. Networks should have Ipv6 or dual stack (IPv4 and IPv6) capability.
Devices to be connected through	PAN	USB, BT, BTLE, NFC, WiFi, ZigBee, ANT.

Table 8-2 – Communication technologies

Scenario	Communication network	Technologies
gateway/data agreegator	WAN	GSM 2G, 3G, LTE; WiFi, CDMA, fixed-line broadband. Network should have Ipv6 or dual stack (IPv4 and IPv6) capability.

Devices in the PAN may be connected to the gateways (aggregation manager) on PAN communication technologies. Smart phone/tablet/laptop may also work as a gateway. Wearable devices may not have the capability of Ipv4/IPv6. It may be considered that all devices/gateways (to be connected directly to public switched telephone network (PSTN)/public land mobile network (PLMN)) should have IPv6 or dual stack (IPv4 and IPv6) capability.

In view of the Internet Architecture Board (IAB) statement on IPv6 [IAB IPV6], IPv4 compatibility may not be available in future developments i.e., in new or extended protocols. Therefore, transition to IPv6 only in PSTN/ PLMN networks will be required in the future. Gateways and devices to be connected directly to these networks will also be required to switch over to IPv6-only capability.

d. Performance criteria

e. Interface requirements

f. User interface

- Physical device: User interface: ON-OFF button, indication of device working status, low-battery indication, device-aggregator connection.
- Aggregator: Communication chanel (e.g., BT, BTLE, WiFi) interfaces. Connection to WAN technologies (e.g., general packet radio service (GPRS), 2G, 3G, LTE, 5G, low-power wide area network (LPWAN)) shall be available, apps can be downloaded (when mobile phone is used as aggregator).
- EHR system interface: App for providing user interface for the data readings, Graphic format for the changes in parameters. Web access to EHR system via user authentication.
- Doctors/Caregiver interface: Providing specific data points with the parameters which are within the range or out of range.
- Government bodies: Web Interface for checking the trends of the patients subscribing to the service.

g. APIs to be exposed to the application from platform

Platform should expose open APIs to all the users, telehealth service providers and infrastructure nodes.

h. Data management

Health data should take into consideration confidentiality, integrity and availability of data. Data minimization should be done as per the related regulations of the country.

i. Data backup, archiving and recovery

The device may maintain the history of the data. Upon transfer of the information to the EHR system, the data may still be available on the local device memory. The oldest data may be overwritten if the device memory is exhausted.

There can be local provision to retrieve the data (e.g., USB connectivity) in case of wireless communication failure. Similarly, a removable memory card can be used for data storage and it can be retrieved for data transfer.

j. Remote device management

Device remote health monitoring and troubleshooting

For most personal care systems, battery charging shall be managed by the user. The device may provide a "low battery" indicator and prompt the user to charge the device or replace the batteries.

Memory management

The device memory management may be done locally. The user or service provider can decide to delete the historical data once the data upload has been done on the EHR System. This can be done using specific applications running on the computer which may manage the memory in secure manner.

In some systems, the service provider may manage the memory of the device.

Device registration and configuration (master-slave, dual master-slave, peer-to-peer)

Each personal health device may have a unique serial number managed by the manufacturer. The device installation or usage needs to be commissioned by way of registering the device for the user and linking it to a EHR system. This is a manual process.

The combination of manufacturer and serial number shall provide a unique-ID to the device. For example, in USB communication systems, the device shall have a vendor-ID and a product-ID and a unique serial number. This is ensured by the manufacturer. The USB consortium assigns the vendor-ID.

The aggregator device shall ensure the unique number in WAN connectivity. This can be mobile phone number when the mobile phone is used as aggregator or the device IP address when using the Ethernet/WiFi connectivity.

k. Startup/Shutdown process

The device's battery life can be monitored remotely for certain devices. This is mandatory for systems where a user cannot charge the device. The data exchange from the device to the server will include the battery status. This enables the service provider to initiate actions for device replacement.

l. Security requirements

Risks related to e-health devices, services and data are well documented [IEEE-ESD]. Health devices, services and data should be protected from known vulnerabilities, take into account nationally identified best practices, and comply with local policies and regulations.

m. Criticality of quality of service (QoS)

RPM deals with patient data that helps in critical decision making and saving patients' lives. Therefore, it is extremely important to have guaranteed response times, have high-end connectivity and backup services to enable seamless healthcare data transmission.

Based on patient data monitoring, analysis and interpretation, medical emergencies and hospital readmissions can be avoided by monitoring patients' healthcare data. Similarly, long-term care of patients' chronic conditions can be well planned with the same.

Criticality of QoS is of high importance in RPM and focus should be on providing high-quality RPM services by deploying the best-in-class healthcare devices, software,

data transmission networks, and high quality clinical staff to provide the clinical interpretation services.

n. Time synchronization

The device may maintain its time locally. The device time should be synchronized with the server by the built-in function. This is a preferred requirement. The local storage of data will be time-stamped using the local time of the device.

If the data is being updated on the server in realtime, the EHR system will record the time as per the server time.

6. Potential market growth

In most countries there is a greater pressure on community care services due to increased life expectancy.

The main established technological solution in homecare services for older people is the personal emergency response system (PERS). It is widely adopted and used throughout most western countries aiming to support "aging safely in place".

Two-way PERS systems are interacting with the use of realtime connection for clinical health measurements which monitor and track an individual's specific medical condition in the home, outside of the four walls of an institutional care setting. This convergence is evolving into a rapidly growing market for RPM and population surveillance.

The global RPM market size was US$703 million in 2015 and is expected to grow at a compounded annual growth rate (CAGR) of 17.0% to reach US$2,130 million by 2022 [AlMR].

According to another market research firm report there was a 44% jump in remotely monitored patients in 2016. It is expected that the number of remotely monitored patients will reach 50.2 million by 2021. Almost half of these patients will be for connected home medical monitoring devices with the remainder coming from personal devices [MobiHealthNews].

7. Implementation constraints (for the support of the use case)

There is a need to manage healthcare needs of large populations in an effective and efficient manner. The following points can be referred as different constraints and challenges:

- High risk/High cost individuals: Adults age 65 and older engage in the highest level of healthcare spending among all age groups. Additionally, almost half of all healthcare spending was used to treat just 5% of the population. Better management of these high risk/high cost individuals outside a hospital setting and in a **preventive care manner** is imperative to lowering healthcare costs, especially as the age structure of the overall population is projected to change greatly over the next four decades.
- In 2010, an estimated 524 million people were aged 65 or older which was 8% of the world's population. By 2050, this number is expected to nearly triple to about 1.5 billion, representing 16% of the world's population [WHO-GHA].
- Managing the growing incidence of chronic conditions: Unquestionably, individuals with multiple chronic diseases place the heaviest burden on the healthcare system. Approximately 80% of Medicare beneficiaries have one or more chronic conditions. Four out of five major chronic conditions that account for hospitalization impact those over 65. Better management of the elderly and their chronic conditions is not a nice-to-have but a must-have requirement. Services for older adults need to be person-centred, coordinated across the continuum of care and focused on health and wellness. Particularly as it applies to 24x7 prevention of acute illness episodes and disease-related disabilities, and where sophisticated, clinically-driven monitoring by population, device

(PERS and "smart" connected health devices) and healthcare constituent (e.g., payer, provider, home care agency).

- Individual coverage expansion (exchanges)/Medicaid expansion: As per data about the USA, about 16 million new enrolees are expected to join Medicaid by 2017. Additionally, the onslaught of expanded coverage across high-risk demographics and the potential for adverse selection on public exchanges will require risk-bearing entities (payers or providers) to look for alternative methods like RPM and monitoring to lower healthcare costs and manage high-risk populations at the point of coverage versus simply at the point of encounter [Health Affairs], [Commonwealth Fund].
- Homecare is not only preferred, but essential: Overall reducing the dependency on institutional care settings has many benefits, including cost savings. Homecare has the ability to play a tremendous role in reducing care spending by treating more people in a cost-effective manner at a fraction of the cost of other institutional settings – in some cases more than 75% lower. Incentives are aligned to promote homecare but also provide the peace-of-mind and safety while living independently.
- Readmission reduction programs: Hospital readmissions for older patients cost American taxpayers more than US$ 15 billion per year – and many are avoidable. Medicare readmission penalties established by US Centers for Medicare & Medicaid Services (CMS) will force both payers and providers to take a fundamentally new approach to coordinating care, particularly post-discharge. This will further incite the demand for RPM and monitoring capabilities to identify risks well before readmission occurrences [JAMA], [YaleNews].
- Consumer/Patient engagement: With patients, caregivers and their family members taking a more proactive role in managing their health, RPM and monitoring is becoming increasingly prevalent in the healthcare industry. In addition to monitoring patients with chronic conditions and senior patients, RPM and monitoring enables patients and their family members to track vital information like blood pressure, weight change, glucose levels and other vital signs while eliminating 90% of the "unnecessary data noise" that is not warranting a clinical intervention. In effect, this means a more prospective monitoring of a patient's health management.

  New smart mobile devices, which provide 24x7 connectivity and extend a broader healthcare value proposition, are filling gaps in care for high risk/high cost patients including the chronically ill. In this view, healthcare challenges are on a much-needed collision course with connected health innovations, including the convergence of PERS and mobility – which is why many industry watchers are optimistic about potential cost savings.

  As this plays out, marketplace spending on these solutions will likely rise – and various market sources are noting that home monitoring systems with integrated communication capabilities are expected to reach 9.4 million connections worldwide, equating to a almost 27% CAGR between 2015 and 2017. In addition, the number of devices with integrated cellular connectivity is projected to grow at approximately 47% CAGR during the same period. Finally, Juniper Research suggests that over the next five years, RPM will result in cost savings of up to $36 billion globally and that North America will account for little over three quarters of the savings.

  Scale and innovation are converging, and the notion of population health monitoring is no longer inspirational – it is real and emerging at the centre of true care coordination initiatives for payers, risk-bearing providers and the cadre of players across the community-based care continuum.

8. Contracts and regulations

   a. Ownership of data

A patient's medical condition data and its derivatives are currently owned by hospitals, healthcare service providers, and healthcare device companies who offer services in various pockets of the country. Confidentiality, integrity and availability of the data need to be taken into consideration.

Many parties owning the data means patients cannot benefit from past health records. There should be a central repository at a patient's disposal for their data.

A patient should have ownership of their data and should be able to authorize other parties involved in their healthcare decision-making such as doctors, nurses, providers, insurance companies, etc.

b. Patient safety requirements

High-quality healthcare devices, tested and certified by various medical and technical organizations, should be permitted. Devices should not harm patients and therefore device testing against electromagnetic interference (EMI)/electromagnetic compatibility (EMC), device safety, device security, technical requirements related to communication technology, specific absorption rate (SAR) (high radiation of frequencies), RoHS, etc., is recommended. This is more important for continuous monitoring devices.

9. Compliance to standards

- ISO EN 13606: Electronic Health Record Communication (EHRCOM).
- ISO 13485:2003: Medical devices – Quality management systems – Requirements for regulatory purposes.
- ISO/TR 14969: Medical devices – Quality management systems – Guidance on the application of ISO 13485:2003.
- HSTP-H810: Introduction to the ITU-T H.810 Continua Design Guidelines.
- ISO/IEEE 11073: Personal Health Data (PHD) Standards. A group of standards addressing the interoperability of personal health devices.
- Continua's test and certification program ensures interoperability by verifying that products conform to the Continua design guidelines and its underlying standards. Certification of sensor devices ensures that IEEE 11073 conformant data is securely received at the gateway. Certification of the WAN interface ensures that each field of every segment in the PCD-01 message contains a valid value. Certification of the HIS interface ensures the syntax and semantics of the XML message [ITU-T HSTP-H810].

8.2 Vehicle emergency call system for automotive road safety

1. Title of the use case

a. Name of the use case: Vehicle emergency call system for automotive road safety

b. ID of the use case: ITS/002/2017

c. Version/revision history: 1.6/ Dec/2018.

d. Source: India/MoC/ TEC

2. Objective of the use case

This use case deals with providing process and infrastructure to automatically call an emergency number in case of a vehicle accident.

3. Background

a. Current practice

Proprietary systems that rely on short message service (SMS) and cellular networks already exist today from certain carmakers. However, standardization of the

communications protocols and of the in-vehicle equipment, thus far, has proved to be the main difficulty in creating common service.

The system uses the driver's mobile phone and is activated the moment the driver enters the car. In the event of an accident, sensors in the smartphone can detect the event and immediately use the hands-free phone capability to connect the driver directly with the emergency service number.

Before initiating an emergency call, the system will provide a time window to allow the driver or passenger to decide whether or not to cancel the call. If not cancelled within the time window, the system continues setting up the emergency call.

The call flow is as follows:

i. In the event of an accident, the vehicle location is determined by the global positioning system (GPS) available in the vehicle or on the phone. Most mid-segment vehicles have factory-fitted navigation systems in them. A driver's smartphone GPS can also be used for emergency reasons. If the GPS is disabled on the phone, the accident event may trigger sensors to activate GPS and then send the location.

ii. Emergency call system announces in the cabin that it is placing an emergency call.

iii. Dials the emergency number for all emergency services.

iv. Automatically plays a message, which informs the operator that a crash has occurred,

v. In a vehicle and the location of that vehicle using appropriate language.

vi. System confirms that the emergency assistance call has been initiated.

vii. The user can cancel the call anytime by pressing the hang-up button.

b. Need for the use case

Every year the number of vehicle accidents and deaths are increasing exponentially.

NOTE – One statistics shows that there are 17 deaths every hour due to road accidents in India [Indian Express]

Lives could be saved by providing support systems, such as ambulances, on an emergency basis. It may be possible if accident information is delivered on time and emergency services are promptly diverted.

Some of the factors affecting the QoS are as follows:

i. Delayed alerts at the emergency centre.

ii. Delayed arrival of emergency services at the accident site.

iii. Insufficient information for mounting a rescue operation.

iv. Inefficient traffic management.

This requires an automated emergency call system in the vehicle that can detect and react when an accident or any untoward incident occurs.

Additionally, the technology presently used is proprietary and limited to only a few models. There is a need for unified standards and policies from governments to have emergency call systems mandated for vehicles.

4. Description

a. Ecosystem description in terms of actors and business roles

The emergency call system is an in-vehicle call system, which opens a line of communication, over GSM/3G/LTE, when an accident occurs. The emergency call

system is positioned in the vehicular network. An accident can be identified based on airbag deployment, fuel pump shut-off, or other abnormal situations arising in the vehicle.

All necessary information required for prompt roadside assistance in time is sent over SMS through an established communication with the emergency service provider.

This includes the following:

i. Geo-coordinates.

ii. Vehicle model and details.

iii. Vehicle diagnostics info for crash impact.

iv. Owner details.

In the event of an accident, communication is promptly started, sharing the location of the accident using the embedded GPS module and vehicle details (preprogramed at the time of production) from the device installed in the vehicle and sharing information from the database having registration details. Vehicle diagnostics information in realtime can be shared from a car area network (CAN) using on-board diagnostic (OBD) device protocol in case the OBD is still working.

A voice call is also placed, allowing the driver to provide additional data to the service provider. However, the voice call is disconnected after a timeout period if the driver's condition is critical.

The emergency call system also publishes the accident information over the V2V network to nearby vehicles and to nearby infrastructure units over the V2I network using short-range communication protocols.

The emergency service provider receives data from the vehicle over the GSM/3G/4G network. The emergency service provider has an intelligent system to analyse received data and then determine the type of service to be deployed at the accident site. The system automatically places a call to the service provider (e.g., ambulance, fire station, car service centre) and shares vehicle data and location information.

Service vehicle deploys an intelligent system, which communicates accident information to nearby infrastructure units, which further forwards the data to other nearby infrastructure units until closer to the accident spot.

Infrastructure units could be signal lights, which receive such data to make way for the service vehicle to reach the accident spot in time, thereby resulting in timely deployment of service vehicle at the accident spot.

Table 8-3 – Actor description

Actor name	Actor type (person, organization, device, system)	Role description
Emergency call system	Device	Device responsible for initiating the rescue operation.
Service provider	System	System responsible for deploying necessary services at the accident site. Arrive at best route for the service vehicle. To communicate accident details to all traffic signals to make way for service vehicles.

Table 8-3 – Actor description

Actor name	Actor type (person, organization, device, system)	Role description
V2V communication Unit	Device	Device responsible for vehicle to vehicle communication.
V2I communication unit	Device	Device responsible for vehicle to infrastructure communication.
Service vehicle	System	Vehicle carrying the necessary equipment.

b. Contextual Illustration

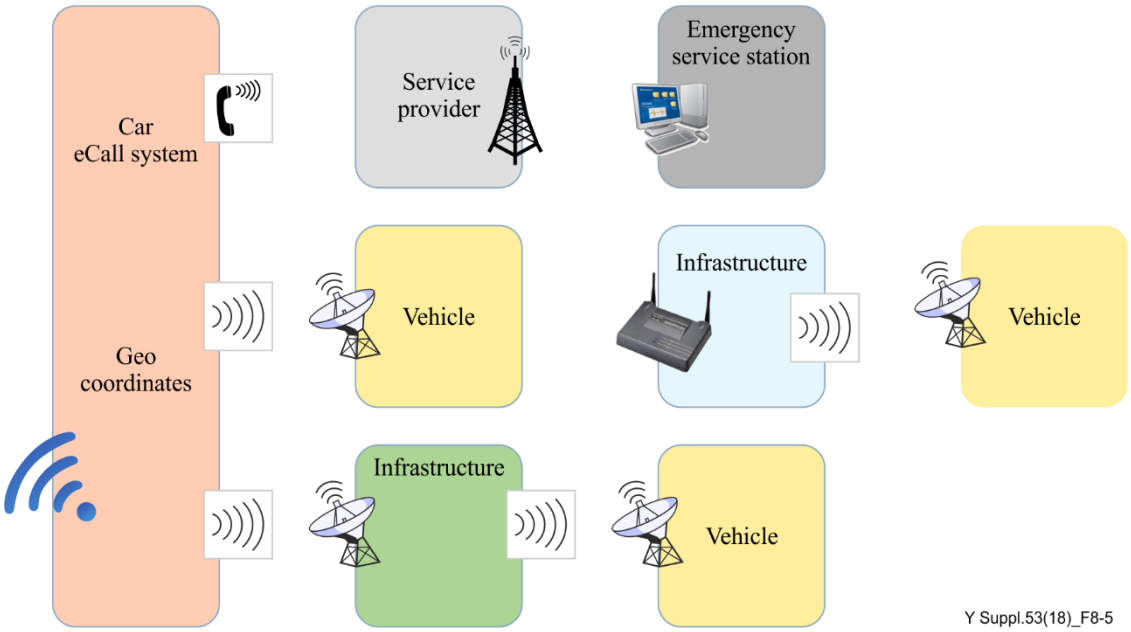


Figure 8-5 – Emergency call system contextual description

c. Prerequisites

The following prerequisites are required to be fulfilled:

- Presence of telecom coverage common routing of emergency calls to an emergency response system.
- Distribution of calls to appropriate emergency response service provider.

d. Preconditions (if any)

The vehicle location tracking device and head-end system should be tested for conformance to local policies and regulations. Local policies and regulations regarding the use of data, including confidentiality, integrity and availability, should be taken into consideration when implementing emergency call systems.

e. Triggers

Any vehicle accident or an untoward accident may activate the vehicle emergency call system.

f. Scenario (generally applicable scenario)

- Some of the challenges anticipated are:

i. Information is sent through SMS for the service provider to identify the nearest emergency service that needs to be promptly deployed at the incident.

ii. If driver has the ability to speak, they can provide additional information for better assistance.

iii. Communication over V2V network is established to communicate accident information with approaching vehicles in the vicinity to avoid secondary accidents and traffic congestion, particularly on highways.

iv. Approaching vehicle to alert the driver about such an incident and further communicate the same to other vehicles in the vicinity.

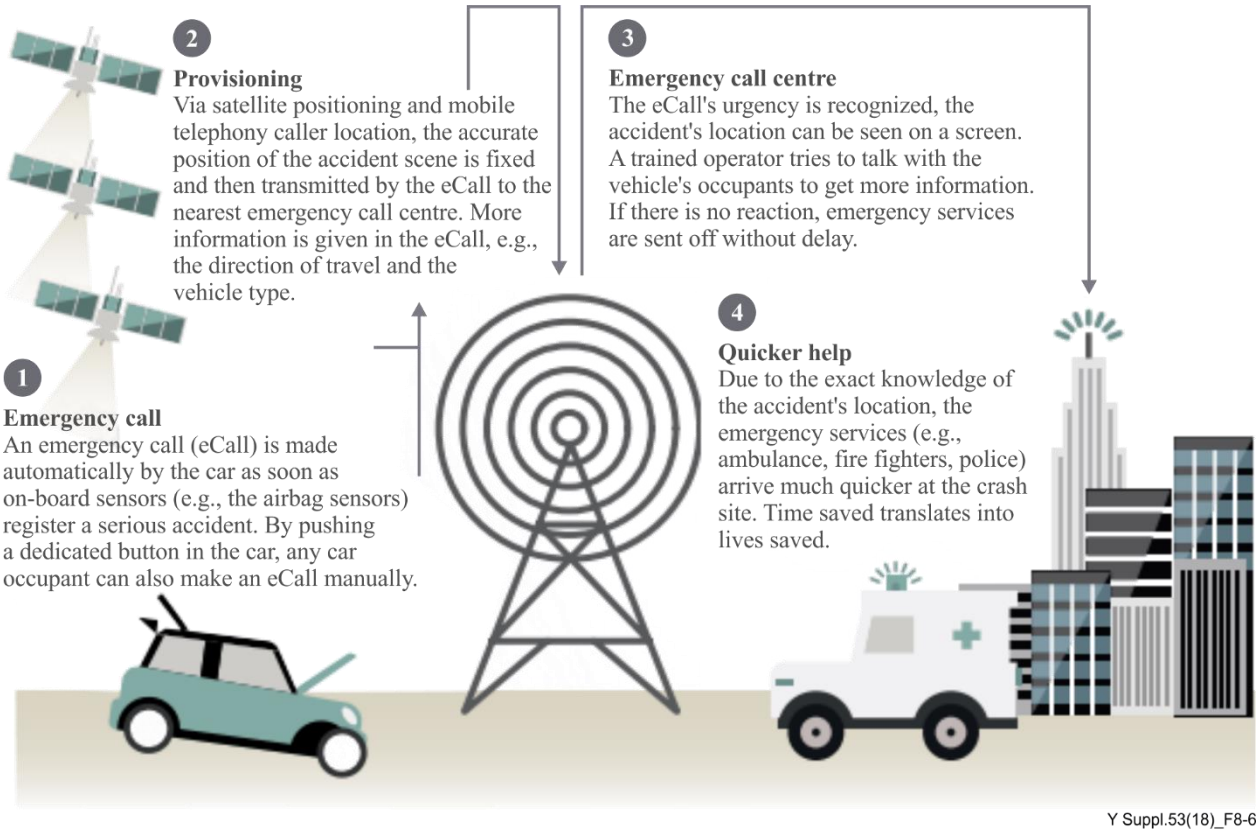
v. V2I network can also be planned to have information flow over a wider range to cover more vehicles.

vi. Emergency service providers to identify emergency services that need to be deployed based on the data received.

vii. Emergency service providers have to promptly arrive, through the best route, for the service vehicle to reach the accident site as soon as possible.

viii. Emergency service providers must communicate the same to all traffic signals in route to make way for service vehicles through the city.

g. Process flow diagram



NOTE – Source [GSMA-mAuto]

Figure 8-6 – Process flow diagram

h. Post-conditions (if any)

i. Information exchange

The emergency call system

- Vehicle identifier tag is the vehicle identification number.
- Vehicle diagnostics information is the OBD data.
- Vehicle geo coordinates are the longitude and latitude details.

Service provider

- Emergency responders are the ambulance service, fire service, car service and police.

V2V communication unit

- Vehicle location (longitude, latitude) details and vehicle type.

V2I communication unit

- Vehicle location (longitude, latitude) and vehicle type.

Service vehicle

- Vehicle location, type, details of owner.

5. Architectural considerations

Architectural considerations, in this clause, are provided for a specific application vertical, but same may also be achieved by adopting an architectural framework having a horizontal (i.e., cross-application verticals) common service layer, which, with standards compliant APIs, may provide common functions (e.g., registration, discovery, group management, security, device management) as a service.

a. Deployment considerations

The emergency call system is to be deployed in the part of the car which the least likely to be damaged in the event of an accident. The device should be to extremely rugged/heat resistant to withstand the impact of an accident. Ruggedness and durability should be similar to that of an airplane's black box.

b. Geographical considerations

Considerations common to different regions [Forbes]:

- Delays are experienced in alerting emergency services.
- Delays are experienced in reaching the accident scene.
- Long rescue times at the accident scene is experienced.

India:

- Infrastructure units are placed a few hundred meters apart from one another.
- Vehicles run on highways at a speed of around 100 Kmph.
- In urban scenarios, traffic is dense with around 1000 vehicles per square kilometers.
- Total of 200 million fleets across India. The road infrastructure is approximately 4.32 million kilometres.

c. Communication infrastructure

The emergency call system is expected to use GSM, UMTS, LTE, CDMA and 5G technologies and other technologies like WiFi and dedicated short-range communication (DSRC). V2V services can also be provided through this network for communication among vehicles.

For addressability, IPv6 or dual stack (IPv4 and IPv6) is expected to be used in all devices/gateways and beyond, which are to be connected directly to PSTN/PLMN.

In view of the IAB statement on IPv6 [IAB IPV6], IPv4 support may not be available in future developments, therefore transition to IPv6 only in PSTN/PLMN networks and gateways/devices to be connected directly to these networks will be required.

Subscriber identification module (SIM) card: A normal SIM card is not suitable for harsh conditions particular to vehicles including vibrations, high temperatures and humidity, and the SIM's life cycle is five years.

An automotive-grade machine to machine (M2M) SIM can tolerate temperatures from −40°C to 125°C and has a life cycle of 15 years. Life of the vehicle is also expected to be 12 to 15 years, therefore an automotive grade M2M SIM, which can be embedded in a vehicle's location tracking device, will work for the complete life span of the vehicle. Embedded SIM [GSMA-SIM] is tamper proof and cannot be removed from the device [ETSI TS 102 671], [Sim Alliance].

d. Performance criteria

   i. Vehicle data, as described above, is transmitted at the instance of an accident from the emergency call system to the service provider.

   ii. Ideally, data should reach the service provider with minimum delay to respond to the situation promptly.

   iii. About 100 bytes of data, which includes geo coordinates, VIN and OBD data is transmitted from the vehicle, over the GSM network, at the time of the accident to the service provider.

   iv. Service provider should dispatch this information to the service vehicle with the problem description upon receiving data from the vehicle at the crash site.

   v. V2V and V2I systems should send vehicle data over vehicular network (dedicated short range communications (DSRC)) at the time of the accident.

   vi. Vehicle data transfer is the highest priority and is the only data transmitted at the time of the accident. In the case of network failure, vehicle data sent over SMS are buffered at the network provider's end, and made available to the end unit as soon as it reconnects with the network.

e. Interface requirements

   Following are the interface requirements:

   i. The emergency call system should be able to receive data from GPS.

   ii. The emergency call system should be able to send data over GSM module.

   iii. The emergency call system should be able to send data over short-range communication interface to approaching vehicle or infrastructure module in the vicinity.

   iv. Service provider shall be able to receive data over mobile network.

   v. Service vehicle shall be able to forward the data to nearby infrastructure unit.

f. User interface

   A graphical user interface-based application is required at the service provider's end and at the service vehicle to view the vehicle's data. No such user interface is required at the emergency call system.

g. APIs to be exposed to the application from platform

   Platform should expose APIs to all vehicle and infrastructure nodes. The APIs should have mandatory fields with optional fields for later use.

h. Data management

   The management of data rate, payload size, frequency of communication, synchronous or asynchronous session types, request, request-acknowledgement, handshake-request, response types, and broadcasts are expected in addition to data integrity.

i. Data backup, archiving and recovery

A six-month data backup of every vehicle should be maintained in active memory. The device should also have the capability to store data and send it to the appropriate platform when connected to the mobile network (in case of coverage holes).

j. Remote device management

Devices should be capable to be configured remotely: Over-the-air (OTA) and firmware over-the-air (FOTA) features should be used. Devices should be upgradable remotely to add new features when required.

k. Startup/Shutdown process

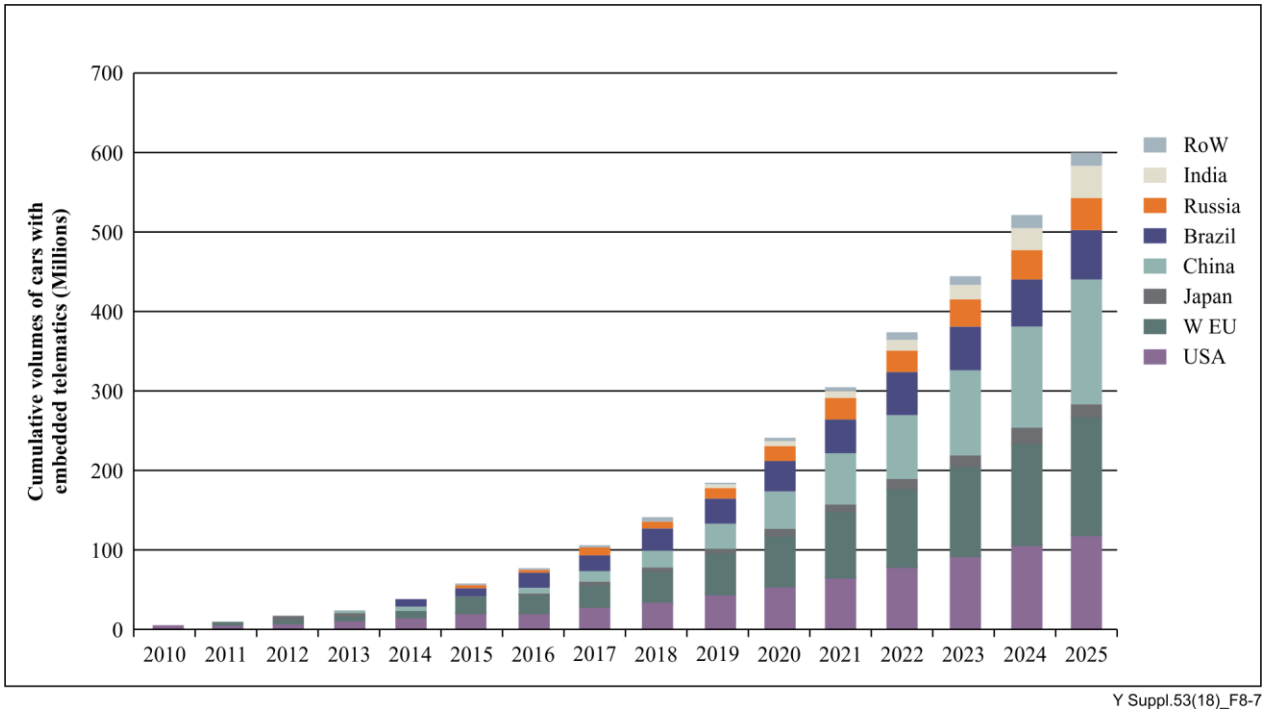
An emergency call system is expected to be battery powered. Once the system is up and running, the device will be in sleep state until an accident event occurs, thereby preventing the battery from draining during normal vehicle operation.

l. Security and safety requirements

Device testing is recommended against EMC, device safety, device security, technical requirements related to communication technology and other requirements (e.g., SAR, IPv6).

6. Potential market growth forecast

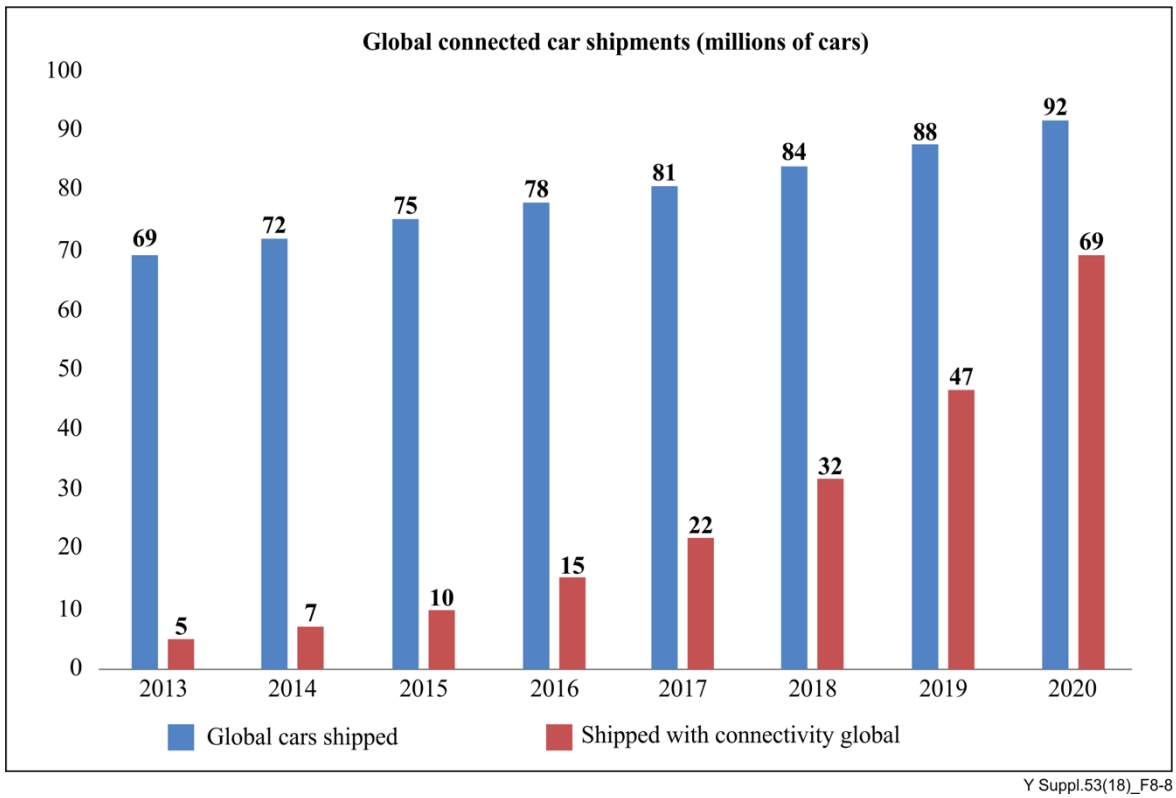
Accelerating growth in embedded, in-car telematics over the next 15 years will lead to cars representing over 5% of all connected devices by 2025, compared with just 0.1% today. The automotive embedded Telematics market will grow at a CAGR of 24.6% over the next 15 years to reach € 20 billion by 2025 [GSMA-mAuto] as shown in Figure 8-7.



NOTE – Source [GSMA-mAuto]

Figure 8-7 – Potential growth

As vehicle manufacturers are adopting sensor technology for monitoring various parameters of vehicles, the data generated may be used by the manufacturer, vehicle owner, user, insurance provider (pay as you drive) and governments, as per their requirement. Figure 8-8 shows a projection of 69 out of 92 million (i.e., 75%) may be global connected car shipments in 2020.



NOTE – Source [4G-America]

Figure 8-8 – Global connected car shipment

7. Implementation constraints

Some of the anticipated challenges are as follows:

i. Frequent presence of multiple emergency service providers for a single geographical area.

ii. Interoperability of different emergency service provider.

iii. Detection of fraudulent calls.

iv. Detection of false alarms.

v. Backup procedures to make calls in case of primary call system failure.

8. Statutory compliances and related regulations

India:

Department of Transportation (DoT) has mandated the number 112 as the common emergency number in line with [ITU-T E.161.1]

All existing helpline numbers such as 100: Police, 101: Fire, 102/108: Ambulance service will be migrated to 112.

Ministry of Road, Transport and Highways, Government of India has released the standard AIS 140 which specifies the conditions and specifications for the use of vehicle location tracking device for the vehicles [ARA-India].

The Bureau of Indian Standards has released a new Standard for Automotive Tracking Device and Integrated Systems (IS: 16833/2018) which mandates the use of the embedded SIM as per the Standards/Specifications of the Telecommunication Engineering Centre (TEC), Department of Telecommunications, Government of India [BIS-India].

NOTE – India has adopted a regime of mandatory testing and certification of telecom equipment. Under this regime, each device having a communication facility is required to be tested and certified

for EMC, device safety, device security and other technical requirements related to communication technology and functional capabilities (e.g., SAR, IPv6) [TEC-MTCTE].

European Union:

The European Union (EU) has issued mandate for a common emergency call (eCall) service 112 for all the European countries.

9. Available global standards

Working Group 15 of the CEN TC274 has written standards on eCall. Compliance with these standards is required in the general approach of the council.

i. EN 16062: eCall high-level application requirements (HLAP) defines the high-level application protocols to facilitate eCalls using mobile networks.

ii. EN 16072: Pan-European eCall operating requirements specifies the generic operational requirements and intrinsic procedures for the provision of an eCall service that allows transfer of emergency messages and to establish a voice channel between in-vehicle system (IVS) and public safety answering point (PSAP).

iii. EN 16102: eCall: Operating requirements for third party support covers the same scope for but for third party services in order to allow service providers to offer services handling eCalls.

iv. EN 15722: eCall minimum set of data (MSD) specifies the content and format of the data to be transferred by the IVS to the PSAP during an eCall.

v. CEN/TS 16454: eCall end-to- end conformance testing sets out test procedures.

The following European Telecommunications Standards Institute (ETSI) standards have been referenced in the various eCall related documents:

- ETSI TS 102 164 (version 1.3.1)
- ETSI TS 121 133 (release 8 or later)
- ETSI TS 122 003 (release 8 or later)
- ETSI TS 122 011 (release 8 or later)
- ETSI TS 122 071 (release 8 or later)
- ETSI TS 122 101 (release 8)
- ETSI TS 124 008 (release 8 or later)
- ETSI TS 124 123 (release 8 or later)
- ETSI TS 126 267 (release 8 or later)
- ETSI TS 126 268 (release 8 or later)
- ETSI TS 126 269 (release 8 or later)
- ETSI TS 127 007 (release 8 or later)
- ETSI TS 151 010 (release 8 or later)
- ETSI EN 301 511
- ETSI EN 301 9

8.3 Digitization and automation of vehicle tracking, safety, conformance, registration and transfer via the application of e-SIM and digital identity

1. Title

a. Name of the use case: Digitization and automation of vehicle tracking, safety, conformance, registration and transfer via the application of embedded-subscriber identity module (e-SIM) and digital identity

b. ID of the use case: ITS/001/16-17

c. Version/revision history (such as no. /month /year): 1.6/Dec/2018

d. Source: India/MoC/TEC

2. Objective of the use case

The proliferation of the embedded SIM and digital identity have made it possible to resolve certain key issues for the connected car, such as safety, vehicular logistics, vehicle registration, transfer, diagnostics and service. This development is very essential, especially for the developing and emerging economies which experience significant concerns relating to compliance, safety and device security within the transport sector.

This use case deals with an approach to enabling the vehicle registration, identification and traceability using technologies such as the M2M SIM (embedded universal circuit card (eUICC)) and digital identity (electronic-know your customer (e-KYC)). The use case can substantially reduce time and cost of the vehicle registration / transfer process and in turn may be helpful in reducing theft and crime.

3. Background

a. Current practice

Most vehicles are fitted with electronic control modules which have support for OBD standard. Vehicle manufacturers are now rapidly adopting the "connected vehicles" paradigm, enabling the vehicles to report events autonomously. The normal SIM card is not suitable for harsh conditions in vehicles including vibrations, high temperature and humidity. Normal SIM card can tolerate the temperature from −25°C to +85°C and its life is of five years whereas the vehicle life is from 12-15 years. Moreover, normal SIM is easily removable, allowing for tampering and fraud.

Although the process of vehicle registration and transfer is done online, the steps for authentication and verification of the owner resulting in linking the vehicle with the owner continue to remain an offline and manual process. After implementation of the use case, the vehicle will get a digital identity which is linked to the solderable SIM identity. This new identity shall be used for purposes of electronic synchronization of the identity of the vehicle and the identity of the vehicle's owner, and also for tracking the ownership and compliance of the vehicle over the vehicle's lifetime. The intervention will make the sale and transfer process of the vehicle electronic, realtime and secure, which will benefit all stakeholders. The vehicle tracking systems which currently use a variety of identities (e.g., International Mobile Equipment Identity (IMEI), device serial no.) for tracking vehicles, will be able to track the vehicle simply by using the vehicle registration number due to its permanent linkage with the solderable SIM identity.

To overcome problems in the automotive sector related to the use of normal SIM cards, the GSM Association (GSMA) has evolved specifications for the embedded M2M SIM, which allows remote OTA provisioning, so that connected devices can be hermetically sealed at the time of production and installed in industrial, hazardous, or remote locations. The GSMA eSIM in solderable form factor is automotive/industrial grade with a life of 15+ years, providing opportunities for auto manufacturers to factory fit connectivity in their vehicles. It can withstand temperature variations for automotive grade, from −40°C to- +125°C. eSIM may store up to five subscription profiles, thereby enabling a selection of bootstrap and commercial life-stages from a variety of mobile network operators

This use case addresses the use of digital identity and embedded SIM for vehicle identification, registration, transfer and tracking using national identity database for the purpose of online authentication of an individual/company/vehicle.

b. Need for the use case

In view of the rapid growth in the automotive sector, especially in developing countries, it is required to digitize the complete process of the connected cars, that will benefit the connected car ecosystem: vehicle manufacturer, vehicle user, vehicle owner, fleet manager, insurer, service agency and the government, to name a few.

c. Country ecosystem specifics

One of the challenges is related to the know your customer (KYC) process for issuance of the M2M SIM.

KYC norms for the M2M SIM used in intelligent transportation systems (ITS) devices (e.g., GPS/GPRS) may be different than the KYC norms for SIMs being used in mobile phones. Currently, there is no mechanism to ensure that vehicle ownership transfer is in sync with the device SIM connection, which needs to be addressed.

- India specific information

Some of the recent developments are listed below:

i. The Department of Telecommunications in India has released guidelines that allow the use of the E-SIM [DoT-India].

ii. The eCall requirement has become mandatory in EU, and the Telecom Regulatory Authority of India (TRAI) has issued a guideline for piloting the eCall in India in its recommendation on M2M in September 2017 [TRAI].

iii. The Ministry of Road Transport and Highways in India has issued a standard [ARA-India] which mandates the use of embedded SIM for commercial passenger vehicle tracking.

iv. The Bureau of Indian Standards has released a new Standard for Automotive Tracking Device and Integrated Systems (IS: 16833/2018) which mandates the use of the embedded SIM as per the standards/specifications of the Telecommunication Engineering Centre (TEC), Department of Telecommunications, Government of India [TEC-MTCTE].

4. Description

a. Ecosystem description in terms of actors and business roles

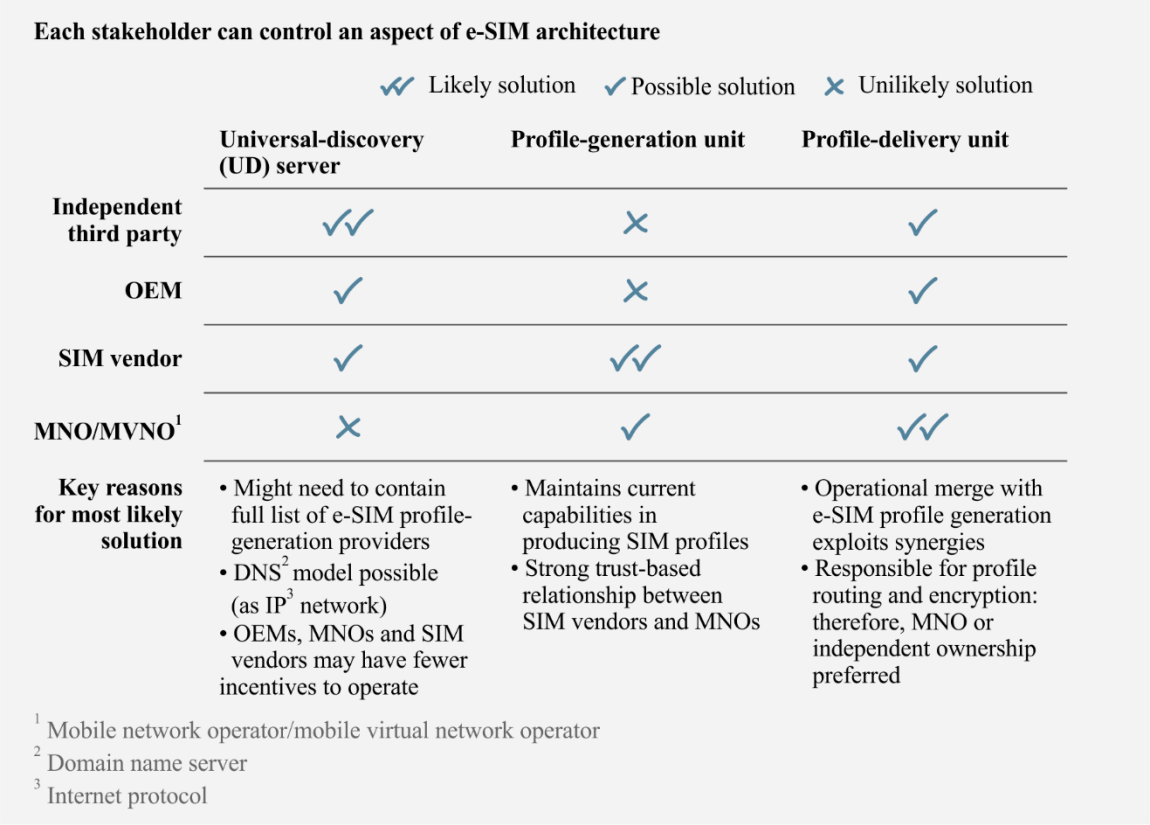
Governments have enacted parliamentary acts to setup national identity registers that can be used for online authentication of citizen identity. Examples are Sweden, France, India (UIDAI), to name a few.

Governments all over the world are pursuing a strategy of digitization and automation to benefit society and also improve governance. The approach presented in this use case enables both of these stated objectives:

- digitization and Automation of the processes connected to registration, transfer and compliance of vehicles.
- use of digital identity (e-KYC) for authentication.

The GSMA embedded SIM business process document "GSMA Embedded SIM Business Process CLP-05-v1-0" defines the role of the M2M service provider as an "Actor who provides services to its subscribers on a contractual basis and who is responsible for the services offered".

The Mckinsey report "E-SIM for consumers- a game changer in mobile telecommunications?" identifies the role of an independent third party for setting up the server for realtime discovery of the subscription profile.



NOTE – Source [ETSI TS 102 671]

Figure 8-9 – Various scenarios of stakeholders in e-SIM deployment

Actors contribute to the ecosystem implementation are listed in Table 8-4.

Table 8-4 – Actors and business roles

S No	Actor	Business role
1	Transport authority	Inclusion of an M2M Identity (mobile number) in the process of releasing vehicles from manufacturing plants; mapping of the buyers e-KYC, mobile identity and the vehicle's M2M identity during the registration of new vehicles; inclusion of the update of buyers e-KYC during the subsequent sale of vehicles.
2	Vehicle OEM	Embedding eUICC during the manufacturing process such that the car goes out "bootstrapped" to a network in the pre-market stage. For vehicles having sensor networks, the OEM may benefit from installing eUICC enabled devices that assist in diagnostics and service management of the vehicle.
3	Device OEM	Device OEMs include support for the eUICC in the in-vehicle telematics, safety and entertainment systems.
4	SIM card supplier	Supplies factory ready SIM cards in MFF2 form factor.
5	M2M service provider	Provider of the enabling provisioning (bootstrap) connectivity and OTA management of subscriptions SIM lifecycle management and e-KYC. This role could be played by a mobile network operator (MNO), virtual network operator (VNO) or a registered M2M service provider.
6	Trust provider	Certification and authentication authority (e.g., national identity registers) that provide online authentication for citizen identification.

Table 8-4 – Actors and business roles

S No	Actor	Business role
7	Mobile operator	The provider of mobile services who must ready their business processes for introducing the eUICC subscriptions OTA.
8	Buyer	The buyer of the vehicle who registers the connected vehicle and links the M2M identity of the vehicle to their name by offering their digital identity for verification and authentication online (e-KYC).
9	Seller	The seller of the vehicle who de-registers the connected vehicle by offering their digital identity for verification and authentication online (e-KYC).

The important Identities and their issuers are shown below:

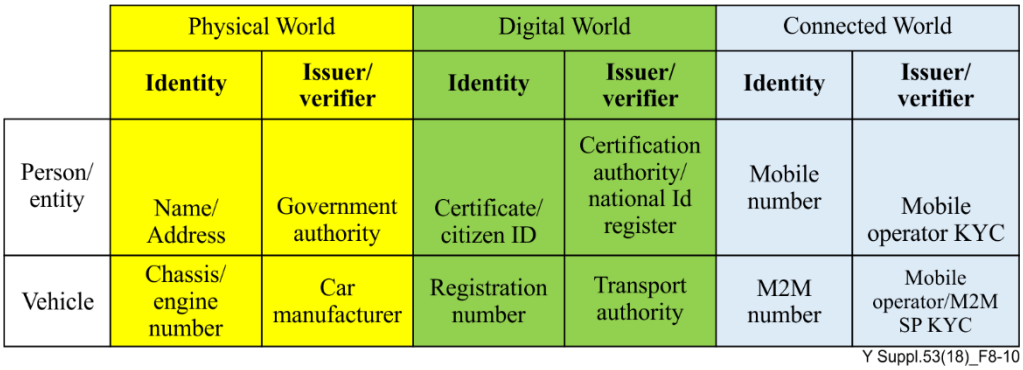


Figure 8-10 – Key identities and issuers

i. Vehicles have a chassis and engine number that identify them in the physical world. Further, a vehicle gets a digital identity when it is registered at the registration authority.

ii. With an embedded SIM, a vehicle gets a new powerful M2M identity (M2M number linked to the eUICC) for the connected world.

NOTE – The M2M Identity can be an IMSI, not necessarily an MSISDN. Whilst it can be argued that MSISDN is not required for M2M use cases, certain countries mandate the existence of the MSISDN for various purposes.

iii. Including a vehicle's M2M identity at the time of vehicle registration can provide a powerful means for realtime identification, verification and contact with the vehicle. This can dramatically change the situation relating to compliance and misuse of vehicles.

iv. Mapping the M2M identity of a vehicle to the vehicle's registration details and the buyer's/owner's mobile identity can substantially increase accountability of the owner, thereby reducing fraud and misuse.

v. The combination of digital identity (e-KYC) and the M2M SIM (eUICC) make it possible for realtime authentication of an owner and buyer and simultaneous realtime update of the vehicle's M2M identity.

vi. The new triplet of mobile identity of the owner, M2M identity of the vehicle and the digital identity of the owner provides a unique triplet with which a vehicle can be remotely accessed and interrogated any time for purposes of vehicle compliance, tracking, safety, convenience and control.

Actors are visualized in Figure 8-11.

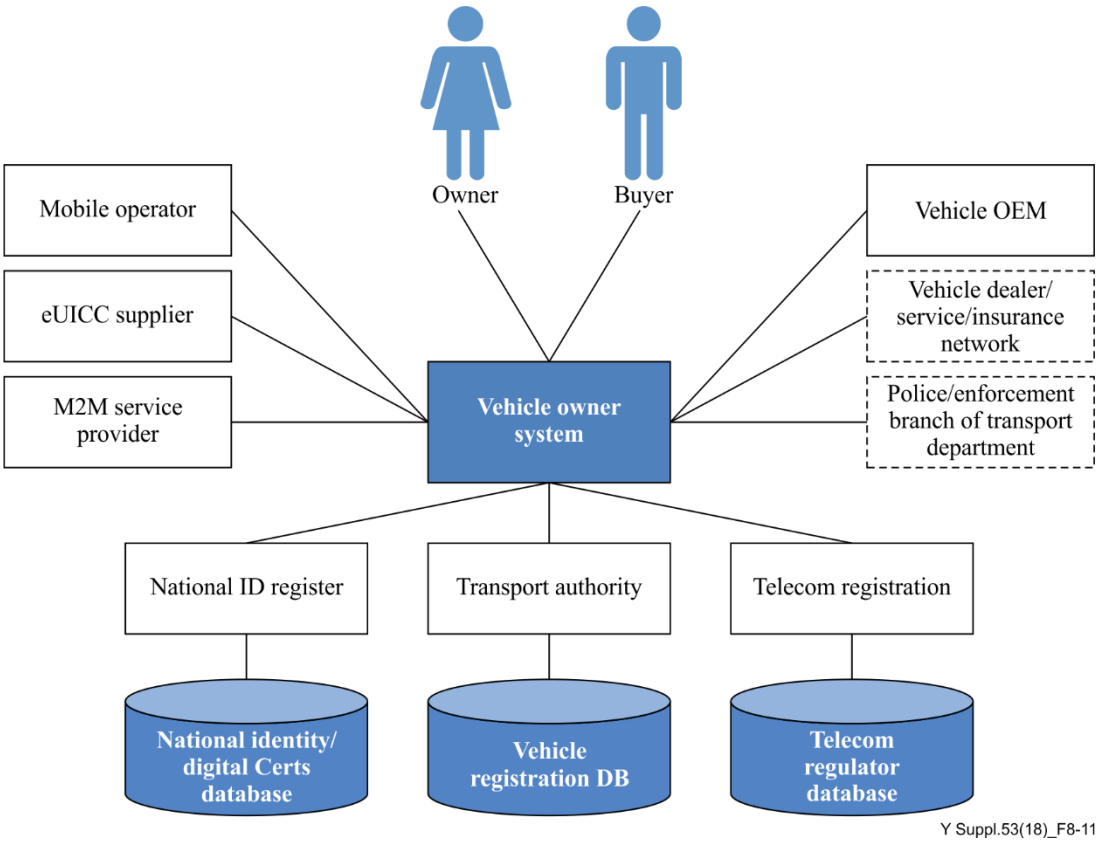


Figure 8-11 – Actors

b. Contextual illustration

Currently, the processes of vehicle registration and transfer passes through several manual steps that require filling out forms and offline authentication and verification of data.

c. Prerequisites

- The prerequisites to implement such a process are defined below:

i. Existence of a national citizen database that provides online authentication of citizen identity.

ii. Vehicles embedded with a remotely programmable M2M SIM (eUICC).

iii. Mobile operator and M2M service provider for enabling and provisioning (i.e., bootstrapping) connectivity and OTA management of SIM and subscription profiles.

iv. Transport authority mandates the requirement to register each vehicle's eUICC at the time of manufacturing, and the registration of the vehicle's M2M identity at the time of vehicle registration.

v. Transport authority mandates the realtime authentication of the buyer using a mobile linked citizen id.

vi. Web interfaces for vehicle registration by the OEM or dealer.

d. Preconditions

- The following preconditions enable the proposed use case:

i. Vehicles are embedded with M2M SIM Card (eUICC).

ii. Securing communication to the connected vehicle such that access is possible from trusted sources.

iii. Securing the access to the data received from the connected vehicle.

iv. The M2M SIM card has a bootstrap connection (provisioning profile) so that the buyer's preferred connection can be downloaded on the M2M SIM card in realtime at the point of vehicle registration.

e. Triggers

- The process flows are triggered from the following events:

i. Vehicle OEM produces a batch of connected vehicle and registers the eUICC with the transport authority.

ii. Transport authority registers a new vehicle in the buyer's name.

iii. Transport authority registers a subsequent sale of a pre-owned vehicle in the buyer's name.

iv. Scrapping of a connected car.

f. Scenarios

- The process can be applied to:

i. New vehicle registration.

ii. Vehicle purchase and transfer process.

iii. Vehicle health, fitness and pollution control tracking.

iv. Vehicle identification.

v. Vehicle location process.

vi. Vehicle fines and tickets recording process.

vii. Vehicle information full (your vehicle).

viii. Vehicle information basic (any vehicle, search by registration plate).

ix. Order new registration plates, order personalized registration plates.

x. Destruction certificate ordering.

xi. Calculate maximum load and trailer weight.

xii. "Suspend" and "Resume" vehicle (fitness/taxation/fines).

xiii. Booking of registration of vehicle (import, or new model).

xiv. Booking of vehicle origination (for imported vehicles, but also procured from army or home-built).

xv. Booking of driver's license test.

xvi. Booking of annual inspection.

g. Process flow

- This process flow describes the car registration and transfer process by the addition of an automation step as described below:

i. The vehicle OEM or dealer enters the vehicle details, along with the eUICC identity online at the point of sale (PoS) or government registration authority at the regional transport office (RTO).

ii. Vehicle buyer mobile identity and digital identity details are entered next.

iii. Vehicle buyer is authenticated using a digital identity or digital certificate if the buyer is a company.

iv. An e-KYC one time password (OTP) is sent to the mobile phone of the buyer (or a digital certificate online authentication for companies).

v. A secure authentication is performed using the M2M identity of the connected vehicle (eUICC can support the most complex authentications, having proven itself as a reliable protection against fraud in GSM networks for more than 30 years).

vi. The registration authority records are updated with the mobile identity of the buyer, the digital identity of the buyer and the M2M identity of the connected vehicle.

The generic actors and associated business roles described earlier in Table 8-4 are clarified below in Table 8-5 in terms of business roles that can be played in an Indian context and a global context.

Table 8-5 – Process actors and associated role takers in the Indian and global context

S No	Generic actor	Business roles in Indian context	Business roles in global context
1	Transport authority	RTO	Vehicle registration authority
2	Vehicle OEM	Vehicle OEM	Vehicle OEM
3	Device OEM	Device OEM	Device OEM
4	SIM card supplier	SIM card supplier	SIM card supplier
5	M2M service provider (M2MSP)	M2MSP	MNO/VNO/M2MSP
6	Trust provider	Unique identification authority of India – UIDAI or digital certification authority e-Aadhaar for individuals or digital certificate-based authentication for companies KYC user agency (KUA)	Citizen Identity
7	Mobile operator	Mobile operator	MNO
8	Buyer	Buyer of the vehicle	Buyer of the vehicle
9	Seller	Seller of the vehicle	Seller of the vehicle

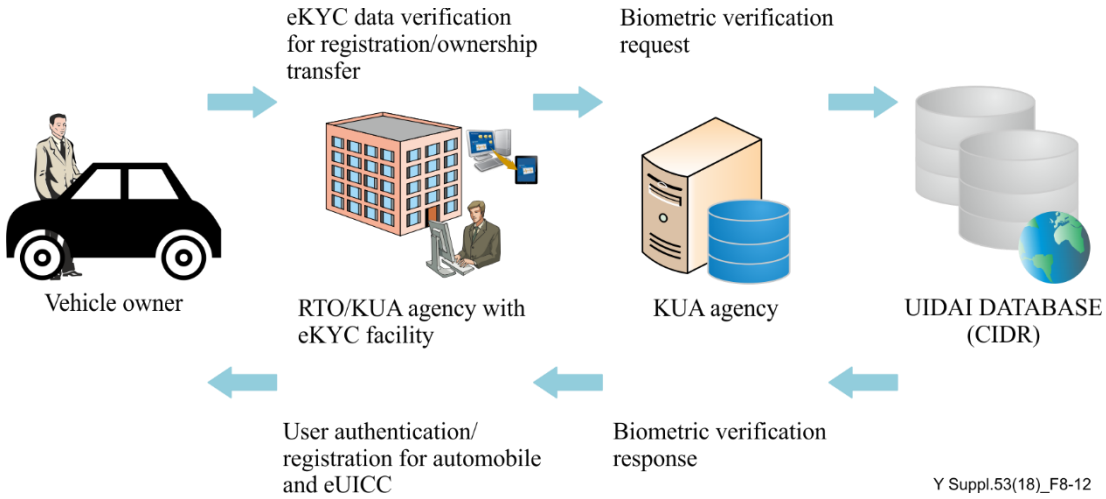


Figure 8-12 – Vehicle registration with e-KYC

The process above, as shown in Figure 8-12, can facilitate the car registration and transfer process including authentication of vehicle owner.

h. Post-conditions

- The vehicle eUICC identity is stored in the transport authority database along with other details about the vehicle.
- The vehicle owner's mobile identity is linked to the vehicle eUICC identity in the transport authority database.
- The vehicle eUICC identity can be used to connect with the vehicle and apps written on the eUICC to authenticate and validate vehicle data for tracking and compliance.

i. Information exchange

- Although the eventual implementation may require additional information flows, the following are the critical ones for a startup use case:
  - i. Communication and registration of the vehicle's M2M embedded SIM with the registration authority.
  - ii. Mapping of the new owner's or buyer's mobile number, e-KYC and vehicle's M2M identity with the registration authority at the time of vehicle registration.
  - iii. M2M device information triplet – device serial No., device communication module identity (IMEI) and SIM serial No. (integrated circuit card identifier (IccID)) linking for bootstrap subscriptions.
  - iv. Connected vehicle engine/chassis and M2M device pairing information.
  - v. New connected vehicle/car production information to transport authority
  - vi. Updated vehicle registration, M2M device information triplet, operational subscription information to transport authority, telecommunications agencies, vehicle OEM, buyer

5. Architectural considerations

a. Deployment considerations

Open API architecture with frameworks having a horizontal common service layer compliant for interoperability between devices, gateways and applications.

GSM module must support IPV6 or dual stack.

b. Geographical consideration

Vehicles with the intended connectivity have mobility within national and international locations.

c. Communication infrastructure

Vehicles factory fitted with embedded M2M SIM (GPRS, 2G, 3G, LTE) working on cellular networks (and where possible CDMA0based R-UIM) with provisioning profiles (bootstrap subscription from a telecom service provider (TSP)/M2MSP) and operational profiles (buyer's mobile subscription).

Provisioning profile for remote provisioning of the embedded SIM throughout the lifecycle of the vehicle.

In view of the IAB statement on IPv6 [IAB IPV6], IPv4 compatibility may not be available in future developments i.e., in new or extended protocols. Therefore, it is necessary that future PSTN/PLMN networks support IPv6 without any assumptions regarding the existence of IPv4 support in the devices or gateways connecting to the network. The networks will indeed require to maintain backward compatibility for existing IPv4 devices for some more time.

d. Performance criteria

High performance, automotive grade telematics device and automotive grade embedded SIM card.

e. Interface requirements

- Interfaces are required for connecting the following devices/systems:

  i. National online authentication systems capable of online verification and authentication of individuals and companies.

  ii. Transport authority systems permitting online vehicle registration and buyer authentication.

  iii. Telematics device ready with embedded SIM and bootstrap connectivity for remote provisioning of the embedded SIM.

  iv. M2M SIM (GPRS, 2G, 3G, LTE) (and where possible CDMA-based R-UIM) for hosting provisioning profiles (bootstrap subscription from the M2M service provider) and operational profiles (buyer's mobile subscription).

  v. OTA subscription lifecycle management platforms.

f. User nterface

- The following user interfaces are required:

  i. Web interfaces for remote profile management of the embedded SIM.

  ii. Web interfaces for vehicle registration, buyer registration, vehicle transfer, compliance check, location enquiry.

g. APIs to be exposed to the application from platform.

Platform should expose APIs to all vehicles and infrastructure nodes. The APIs should have mandatory fields with optional fields for later use.

h. Data management

As per industry standards.

i. Data backup, archiving and recovery

As per industry standards.

j. Remote device management

Web interfaces for remote profile management of the embedded SIM and the remote device management.

k. Memory management

The embedded SIM memory management shall include functions that enhance the memory life to 12 years; see clauses 5.9, 5.1 of [ETSI TS 102 671].

l. Startup/Shutdown process

As per industry standards.

m. Security requirements

Embedded SIM cards developed as per the relevant ETSI and GSMA guidelines.

Remote provisioning as per relevant GSMA guidelines.

n. Criticality of QoS

- To enable QoS in automotive use cases, the following recommendations are proposed:
  - i. Vehicle fitted with embedded SIM having a primary and fallback subscription to maximize QoS connectivity in all locations.
  - ii. Automatic switching of networks in the embedded SIM to enable high QoS.
  - iii. Heartbeat monitoring of the connectivity and remote switching of subscriptions profiles for ensuring connectivity in local and roaming PLMNs.

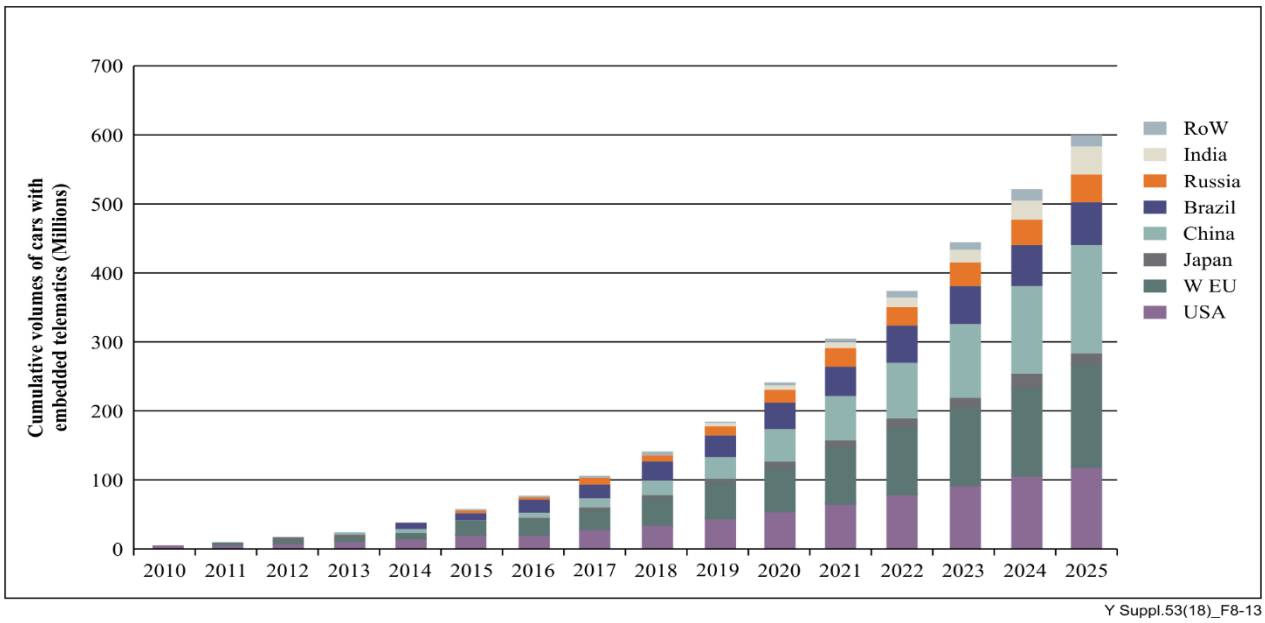
o. Time synchronization

As per industry standards.

6. Potential Market Growth

Connected Vehicles are set to drive the adoption of M2M globally.

Accelerating growth in embedded, in-car Telematics over the next 15 years will lead to cars representing over 5% of all connected devices by 2025, compared with just 0.1% today. The automotive embedded Telematics market is expected to grow at a CAGR of 24.6% over the next 15 years to reach €20 billion by 2025.



NOTE – Source [GSMA-mAuto]

Figure 8-13 – Connected vehicles forecast

A recent McKinsey report says the following regarding the M2M enablement with the e-SIM:

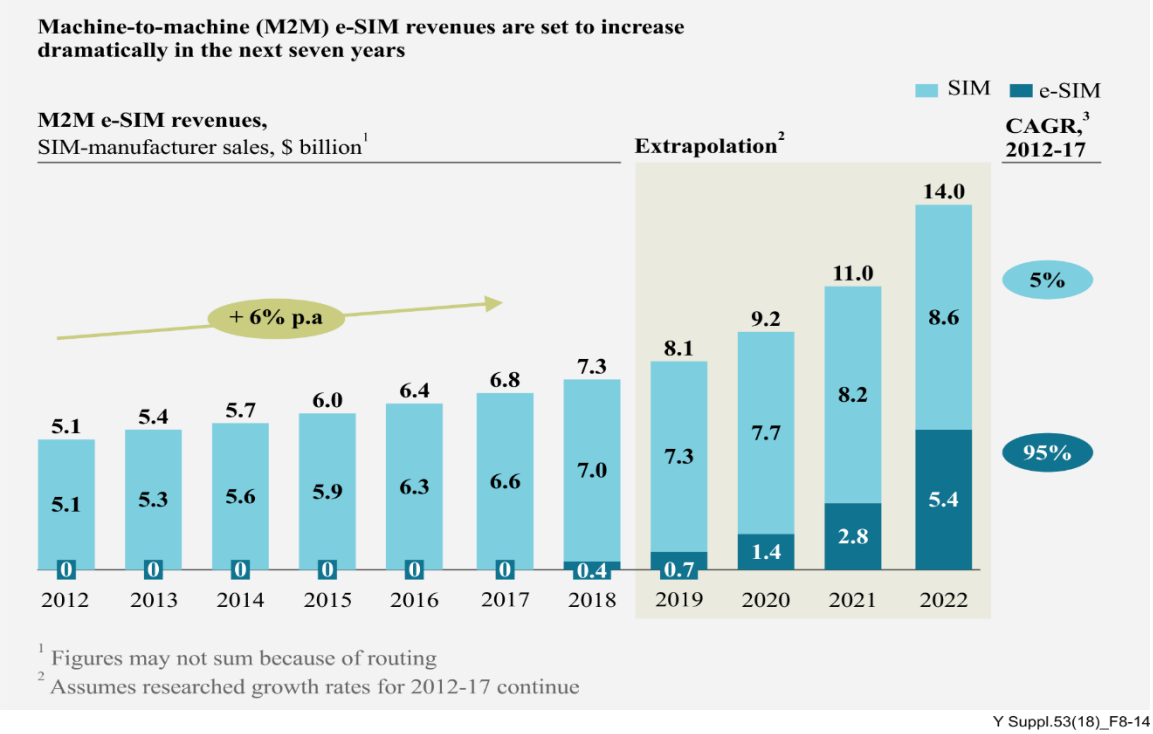


Figure 8-14 – McKinsey Research, Jan 2016

7. Implementation Constraints

The following implementation constraints are visualized:

- Mandating the standards for telematics devices;
- Policy mandates for the M2M service provider;
- Open API for transport authority databases for online registration and authentication;
- A national identity database which offers online authentication.

8. Standards, Statutory compliances and related Regulations

The following related documents are noted here:

i. GSM Association Non-confidential Official Document SGP.02 – Remote Provisioning Architecture for Embedded UICC Technical Specification.

ii. Digital identity: Digital Identities provided by Government Root Certification Authorities such as the Controller of Certification Authority in India or other trust providers with non-repudiation capabilities such as the Unique Identification Authority of India (UIDAI).

iii. Regulatory compliances are required before implementation.

iv. Transport authorities, responsible for registration of vehicles seem to be active in connected vehicle scenario. As an example, Ministry of Road Transport and

Highways in India has released [ARA-India] which specifies the conditions and specifications for the use of connected devices in vehicles.

v. Some security standards inOneM2M specifications, which are relevant to this use case, point to the use of eUICC in the following roles:
   – providing trust for application level security in addition to the network authentication within GSM/3G/LTE/Mobile-IoT networks;
   – providing trust for application level security within non 3GPP networks;
   – as a secure element for all M2M gateways and M2M nodes.

vi. Certification by accredited test houses.
   – it is recommended that location tracking devices are tested and certified by a Test House accredited by the relevant SDO/statutory standardization authority before deployment in the network;
   – by example, India has adopted a regime of mandatory testing and certification of telecom equipment. Under this regime, each device having a communication facility is required to be tested and certified for EMC, device safety, device security and other technical requirements related to communication technology and functional capabilities (e.g., SAR, IPv6).

9. Digital identity available global standards

- [ETSI TS 102 225];
- [ETSI TS 102 671];
- [ETSI TS 102 267].

For all other relevant standards for the smart cards, refer to [ETSI Smartcards]; for SIMs, refer to [ETSI SIM].

- [oneM2M TS 0002].

For all other related oneM2M specifications, see [oneM2M Drafts].

The following relevant updates in the oneM2M standard [oneM2M TS 0002] are reported for this use case:

SER-00	In case where the M2M Devices support USIM/UICC and the Underlying Networks support network layer security, the oneM2M System shall be able to leverage device's USIM/UICC credentials and network's security capability e.g., 3GPP GBA for establishing the M2M Services andM2M Applications level security through interfaces to Underlying Network.	Implemented in Rel-1
SER-005	In case where the M2M Devices support USIM/UICC and the Underlying Networks support network layer security, and when the oneM2M System is aware of Underlying Network's bootstrapping capability e.g., 3GPP GBA, the oneM2M System shall be able to expose this capability to M2M Services and M2M Applications through API.	Implemented in Rel-1
SER-006	In case where the M2M Devices support USIM/UICC and the Underlying Networks support network layer security, the oneM2M System shall be able to leverage device's USIM/UICC Credentials when available to bootstrap M2M Security Association.	Implemented in Rel-1

- Universal Mobile Telecommunications System (UMTS); Service aspects; Service principles (Release 8 or later);
- (Release 8 or later);
- (Release 8 or later);

- (Release 8 or later);
- (Release 8 or later);
- (Release 8 or later);
- (Release 8 or later);
- (Release 8 or later).
- General remarks
    i. The trilogy of the M2M SIM, digital identity (electronic KYC) and the role of the M2M service provider have the potential to dramatically change the M2M enablement scenario for the industry.
    ii. The concept of machine KYC [TRAI] is fast becoming relevant, especially in the backdrop of remote connected dispersed and mobile assets such as vehicles, meters etc. It is not sufficient to know the identity of the owner (person) of the connectivity element, but equally important to know the machine the connectivity element is fitted in. Governments may consider the need for a trust centre, that can identify machines based on tamper resistant connectivity elements, such as to add security and safety to the IoT use cases.
    iii. To ensure mandatory factory fitment of connectivity with automotive grade hardware, tamper-proof security in the connectivity element, multi-market support for MNO connectivity with remote provisioning, it is recommended that the MFF2 (solderable) eUICC be considered in the development process of standards for automotive tracking and emergency call requirements. Further, MFF2 (solderable) eUICC is expected to benefit the unique identity and online registration of vehicles, as the solderable connectivity element may be used for the purpose of vehicle identity and authentication. The implementation of the embedded SIM and remote provisioning should consider compliance with the GSMA guidelines including the SAS certification.

8.4 RFID-based digital identification for vehicle tracking, registration and data transfer

1. Title
    a. Name of the use case: radio frequency identification (RFID)-based digital identification of vehicles for tracking, registration and data transfer
    b. ID of the use case ITS/002/16-17
    c. Version/revision history: 1.0/September/2017
    d. Source: Egypt/NTRA; Nigeria, Senegal, Ghana, Burkina Faso, Tunisia, Algeria
2. Objective of the use case

The identification of vehicles is considered an essential aspect to ensure accountability and safety, and to also streamline all logistical and management aspects related to vehicles registration and driving licensing processes. Vehicle number/license plates (N/LP) are currently an effective means to identify vehicles all over the world. However, N/LPs are subject to damage, theft, and due to, for example weather conditions, they could show delamination or other effects which might yield the plate unrecognizable, or illegible.

Using secured and physically-associated digital identifier which would be robust against tampering, data modification, and any type of physical and/or information attacks are thus needed to establish a digital infrastructure connected to the vehicles, to aid in vehicular logistics, registration, ownership transfer and tracking scenarios.

This use case is very crucial, to streamline compliance with safety regulations within the transportation and logistics sector of many countries.

3. Background

a. Current practice

All registered vehicles are fitted with N/LP satisfying specific plate requirements and standards. These standards are set by the administrations to ensure an optimized legibility to the human eye. Additionally, special design measures can be applied to increase the reliability of automated license plate readers (ALPRs). N/LPs play a vital role in preventing and solving crimes. Misreading the N/LPs could lead to a high degree of damage and accordingly, consistent efforts are being done to increase the legibility of the plates and increase its durability and resistance to different forms of attacks and conditions.

The process of vehicle registration and ownership transfer today, passes through several manual or automated steps depending on the variance between the countries in different region of the world. Manual processes which implies the manual purchase of registration, inspection and compliance forms, in addition to the manual authentication of the identity of the drivers, vehicle and essential vehicle parts (i.e., motor) are done through human operators.

This is prone to error, and in some occasions, failures to comply with safety regulations; which pose a threat to the drivers and the community as a whole.

b. Need for use case

Employing a secured and fast means to uniquely identify vehicles, is of extreme importance in the transportation sector. The necessity of having an interoperable system and architecture that easily integrates with city management platforms and other IoT related systems and services highlights the need to specify a use case for RFID based digital identification of vehicles for tracking, registration and data transfer. Potential beneficiaries include transportation authorities, law enforcement agencies, insurance companies, health agencies and the users themselves to name a few.

c. Country ecosystem specifics

RFID regulations are subject to the radio regulations specific mandates in each administration, with respect to power limit and operating bands.

4. Description

a. Ecosystem description in terms of actors and business roles

In order to harmonize the use case to be suitable to the maximum number of administrations possible, a generalization for the key roles is conducted and a harmonization for the potential business roles is proposed. It is generally understood that country specific variations for key actors in the system, are to be expected. The following represent a high level description of key actors and their roles:

- Government authorities: includes official governmental authorities responsible of the vehicle registration and compliance management processes. They may include law enforcement agencies, transportation authorities, municipalities, governmental associations or any other agency or institute responsible of setting regulations and testing for compliance, and conducting auditing and checking for the identity of the vehicle and its parts;
- End-user: includes the car owner, usually complying with set regulations and providing necessary documentation to prove his/her ownership/ legitimate possession to the vehicle;
- Technology providers and systems integrators: includes vendors and manufacturers of the key system components which include RFID readers, tags, antennas,

information systems for different applications (i.e., tolling, tracking, vehicle identification, etc.);

- Licensed operators/service providers: includes providers of backhaul connectivity between the different RFID information system elements for a more connected and integrated system, employing say cloud-based solutions;
- RFID operators: Depending on the application at hand, operators could be private entities, or public administrations operating the system to realize some specific applications like tolling, logistics, etc.

b. Contextual illustration

The following contextual illustration displays the key stakeholder groups and their roles:

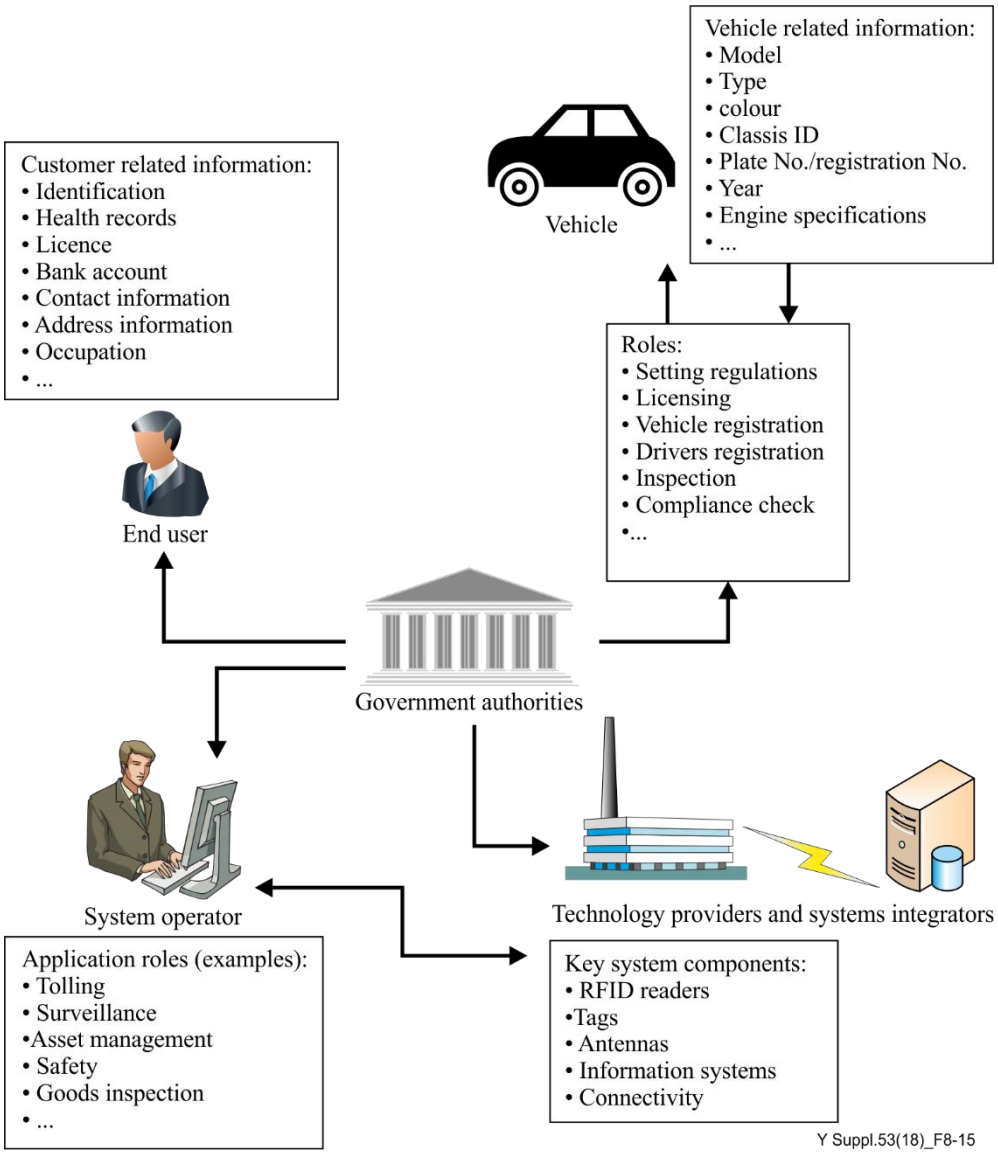


Figure 8-15 – Contextual illustration of key stakeholders' groups and their roles in RFID based digital identification of vehicles for tracking, registration and data transfer

c. Prerequisites

- adopting a national unified identification scheme across all vehicles (e.g., EPC, etc.);
- testing of RFID tags, and ambient environment for the readers to check the system performance and noise/interference immunity;

- availability of frequency spectrum and properly set regulations (e.g., EIRP power levels) in accordance with best practices, international standards and application;
- digitization of end user identification national registry and automation of the whole process of vehicle registration management, inspection and compliance processes.

d. Preconditions

- tags should be read many, write once, self-destructible in case of removal, complying with the standards available in the industry.

e. Triggers

The processes flows are triggered from the following events:

- RFID vehicle identity registration process;
- vehicle identifier query process;
- revocation process;
- automatic payment process;
- clearing house process;
- customer service process.

f. Scenarios

The above-mentioned processes can be applied to the following scenario:

- Plaza tolling and/or checkpoint scenario:

  All vehicles are registered to the system at their license renewal date. The drivers are allowed to open a bank/service account with their personal and their vehicle information. Drivers all given the option to either provide their credit card details, or open a prepaid bank/service account for some services like tolling. Every vehicle will have a tag (RFID) with a unique tag identification number.

  A vehicle approaches a plaza tolling station. In some situations, there may be a need to combine the plaza with additional checkpoint, subject to the laws and regulations in different countries.

  The system checks the vehicle for the presence of an RFID tag, and if present, the vehicle is queried for its identification information and licensed drivers' details. A check is performed according to the laws and procedures set in the different member states. If the vehicle is clear to pass, the system checks if the former has an associated bank/service account related to the tolling application. If there is enough credit, and/or depending on the service plan of the customer, the vehicle is allowed to pass, deducting the toll value from the customer's account.

  In case only tolling applications are implemented, the system checks the vehicle for the presence of an RFID tag, and if present, the vehicle is queried for its identification information and licensed drivers details for authentication purposes. If the vehicle account has enough credit, and/or depending on the service plan/agreement of the customer, the vehicle is allowed to pass, deducting the toll value from the customer's account. Else, the vehicle is directed to the normal manual tolling lanes.

  System malfunctioning and/or errors in toll collection value, or account balances can be reported through the customer service platform/process.

  The clearing house is used to settle financial transactions between the different stakeholders in the system, including for example, the banks (service account), the authority managing the tolling plaza and other agencies.

  Customers can recharge their accounts using top up cards, prepaid cards which they can purchase from different retails stores.

g. Process flow

5. Architectural considerations

a. Deployment considerations

The following considerations are considered mandatory:

- the deployment model is deployment at once;
- the interoperability of system devices and compliance with relevant standards at the onset of the deployment phase must be in place;
- interference analysis shall be conducted to make sure that the readers will not be affected by existing radio services operating in the vicinity of the plaza.

b. Geographical consideration

The following considerations are considered optional subject to the requirements of each administration:

- tolling plazas should be placed along key inspection points, and/or highways and travel ports.

c. Communication infrastructure

A fully reliable and always connected communication infrastructure between the plazas and the information system servers are needed to make sure that realtime information is available during the query process. Ultrafast broadband connection may be needed if a combined LPR system is used in conjunction with the RFID vehicle identification system.

d. Performance criteria

Criteria related to the following categories are envisioned:

- RFID related performance criteria:

  RFID related performance criteria depends on many factors such as location of tag in the vehicle, vehicle speed, tag and reader location, and use of multiple tags per vehicle for achieving higher accuracies. Recommended placement of tags differs based on the scenario of system implementation. However, in principle, better results are achieved by placing the tags under the windshield, and the readers/antennas above 4 ft from the ground. The performance results though would depend on other important factors like the presence of multiple tags from different vehicles in the vicinity of the reader, and the type of windshield used (for example insulated glass), which may impact the performance of the system. These considerations have been supported by studies as illustrated in [Nash 2016].

- Information systems related performance criteria:
- Connectivity performance criteria:

e. Interface requirement

Standardized interfaces are to be adopted in the solution.

f. User interface

A web-based interface is to be provided for all system processes mentioned in clause 4, part (e).

g. APIs to be exposed to the Application from platform

h. Data management

i. Data backup, archiving and recovery

j. Remote device management

k. Startup/shutdown process

l. Security requirements

The solution shall implement encrypt all stored and exchanged information on and between tags, and the information database holding the queried information.

8.5 Connected smart home

1. Title of the use case

   a. Name of the use case: connected smart home

   b. ID of the use case: home automation/001/17-18

   c. Version / revision history: 004/Dec/2018

   d. Source: India/MoC/TEC

2. Objective of the use case

   This use case describes a cost-effective smart home solution that can be integrated with "Smart City Services" to elevate the lifestyle of citizens.

   The solution service provider should take complete responsibility of deployment and maintenance of the system, covering all of the key areas of the ecosystem, including hardware, software and services.

   Uninterrupted supply of utilities such as power, water, gas, etc. may be ensured by third party public and private service providers associated with the smart home solution.

   In the smart home scenario of this use case, home owners can monitor and control IoT devices locally or from remote locations in a hassle-free, reliable, secured yet cost-effective manner and get timely alerts in emergency situations.

3. Background

   a. Current practice

      One of the major inhibitors in implementing home automation system is lack of required infrastructure.

      Home owners interested in deploying a smart home solution, either hire a solution provider or procure and install do-it-yourself (DIY) home automation kits. Although some of the solution providers design their own hardware components, many others pick and choose readily available components from the market.

      Most connected home vendors focus on one or two categories of products or services. Also, typically vendors do not engage with home owners once the installation is completed. From the home owner's prospective, home automation system upkeep takes a low priority, unless the home owners' past experience has led them realize real value from the solution. This situation may result in homes where the system becomes non-functioning over some period of time.

   b. Need for the use case

      With rapidly changing lifestyles, there is a growing need for home automation solutions. The main reasons for deploying home automation solution include the desire for safety, convenience, comfort, energy saving, etc.

      In smart city projects initiated by governments or integrated townships, a connected home becomes a part of the ecosystem consisting of (but not limited to) numerous city assets such as utilities, transportation, healthcare, law enforcement, waste management, etc. By becoming a part of the larger ecosystem, smart and connected homes can help the entire ecosystem function more efficiently and seamlessly.

      Smart home/home automation systems should be viewed as building blocks to build smart cities. In addition to providing abilities such as controlling appliances remotely, a smart home should integrate with external systems and help the residents in different

aspects of life, such as managing day to day chores, to maintaining safety, to providing support system during natural disasters.

As an example, the home automation system may handle periodic utility payments via a registered payment gateway to the appropriate utility provider, post approval of the resident. Or, with the help of features like image recognition, the system can alert the local emergency authorities about abnormal patterns in the neighbourhood. Or for government agencies, the system may provide a faster outreach to a wider population in cases of natural disasters such as typhoon or storms.

In the view of Society 5.0 [Society-5.0], which by definition is "A human-cantered society that balances economic advancement with the resolution of social problems by a system that highly integrates cyberspace and physical space", new technologies such as IoT, AI and big data can play a significant role in improving the quality of lives [Society-5.0].

Apart from providing personalized services to the home owner, smart home solutions should be targeted to assist the individuals with special needs. For instance, in an old age home, the residents may be able to control the appliances using voice commands. This may be achieved with the help of readily available off the shelf appliances. Similarly, a speech-impaired individual may be able to control the necessary functions with the help of gestures.

The most effective goal behind implementing smart and connected homes solutions could be to leverage the technology in order to provide an equal opportunity to individuals with disabilities.

c. Roadblocks in leveraging full potential of home automation solution

With the steady growth in wearables, home entertainment and bring-your-own-device (BYOD) trends, home owners and at times even solution providers, select components from a plethora of proprietary smart appliances to create home automation system. This, however, results in creating an intricate application rather than a purposeful solution. Although, such systems may allow home owners the means to control a set of smart appliances, they usually fall short in the area of analyzing and providing valuable statistical data in a usable format to home owners. Such solutions typically work in silos, failing to take advantage of the overall IoT ecosystem described in an earlier clause. Using smart appliances from different vendors poses yet another problem. Each appliance usually is bundled with its own proprietary application. Managing a multitude of such devices becomes challenging for home owners. For example, a seemingly-simple configuration change such as updating the phone number to receive alert messages, will require the user to make changes for each appliance separately.

Connected home devices and solution vendors need to prove their reliability before they can break into the mass market. Fragmented ecosystem, price and perceived value, lack of high-speed reliable network coverage and interoperability between disparate network technologies that are still evolving are seen as roadblocks in quick adoption of home automation solutions.

d. Proposed approach

The proposed home automation approach will allow home owners to remotely monitor and control IoT devices, and receive alerts via the gateway installed inside a house. A home owner will be able to take cognizance of an unannounced visitor by streaming images from a surveillance camera attached to the doorbell at a remote location. Emergency alerts requiring immediate attention will be sent not only to the registered home owner but also to concerned third parties such as emergency office, healthcare provider or fire brigade via a call centre/provider network. The system can solicit home

owner's consent before notifying third parties. Rules to raise alerts and send notifications will be configured through a rule engine, provided by IoT platform.

For the home owner's convenience, the responsibility to upkeep various IoT enabled devices inside the house will be handled by service provider's call centre. The gateway will monitor health of IoT devices such as smart switches, smoke/gas detector, motion sensor, beacons, microphone, siren, etc. and inform the call centre when an IoT device has to be repaired or replaced. This model will ensure that the home automation system takes the hassle of maintaining the system away from the home owner.

Communication between the gateway and the home owner and between the gateway and the cloud server will be carried out over secured channels. Users will also be able to monitor multiple homes, provided each home has its own gateway. Additionally, one home can be managed by more than one family members.

The system will provide analytics and reports such as overall/monthly energy consumption, usage of various home appliances, statistics of various alerts, etc. to home owner. Communication with third party agencies will be handled by the platform administrator using various communication channels.

The system will provide customized weather alerts or configure wake-up alarms based on the family members' calendar along with other parameters such as preferred mode of transportation, weather, etc.

To develop smart cities based on smart home systems as building blocks, different agencies (government and private sector) would need a standardized mechanism to publish their services to any home automation provider. Private agencies may also be able to monetize their value- added services with such systems.

The proposed smart home will also learn from the habits of the family members and pre-emptively act by itself or upon manual confirmation and control the home appliances or provide the necessary voice guidance.

e. AI and edge intelligence in home automation

Prevalent home automation solutions are limited in their capabilities and revolve mostly around the ease of monitoring and controlling electrical equipment remotely. However, certain areas such as safety, device security and compliance requirements demand intelligent edge devices. These requirements can afford neither the communication failures nor the communication delays. For instance, an algorithm to detect suspicious activity based on video analytics is geo specific and also needs to be executed without any delays. Such solutions require elements of edge intelligence.

The smart home solutions should leverage machine learning algorithms to recognize various patterns such as energy utilization and inhabitant's behaviour in order to provide comfort, safety and optimum resource utilization. For example, based on connected appliances and energy utilization patterns, it can be possible to identify and even predict the possibility of failures. A self-learning home is envisaged, which will learn based on ambient conditions and user's actions, and either recommend actions or execute actions with appropriate permissions.

f. A typical use case fulfilled by the proposed approach

An individual may own multiple properties in different geographic locations; in this case, it may be difficult for the owner to be aware of the property health for all properties from a remote location. Property health can be defined as availability of utilities such as water or electricity and home appliances in working condition.

This approach will:

- enable home owners to perform various operations remotely. Remote operations are especially useful for appliances such as water pump, which can get jammed if not used on a regular basis;
- help keep the home in functional condition by keeping the owner informed about the status of appliances;
- send emergency alerts to the owner as well as to the concerned third parties in case of incidences such as fire, break-ins and flood;
- provide essential third-party services to the family members. For instance, in case of a medical emergency, the gateway can be used to contact nearby ambulances or hospitals either directly or via a call centre;
- periodically provide usage history of utilities, in order to avoid unpleasant surprises at the end of billing cycle and help detect miscalculations in billing, if any. In the future, the home automation gateway may also be integrated with utility providers and a payment gateway to make utility payments; relieving the property owner of such regular chores.

4. Description

a. Ecosystem description in terms of actors and business roles

The solution involves an Internet enabled gateway, service provider (or call centre), TSP, IoT platform, owners' smartphones or tablets, third party services, society/community/city office (optional) and of course the home owners. Table 8-6 lists relevant actor descriptions.

Table 8-6 – Actor description

Actor Name	Actor Type	Role Description
Internet enabled Home Gateway	Device	Hardware device facilitating communication between IoT enabled devices and the platform. May provide HMI (Human Machine Interface) for home owners to control and configure IoT devices. Interprets local rules to perform critical actions such as switching off long running appliance.
Home Owner	Person	Main stakeholder. Manages and controls various aspects of real estate property.
Service Provider/Call Centre	Organization	Facilitates services on behalf of the home owner.
TSP	Organization	Provides telecommunication network infrastructure for home gateways and owners' smartphones to communicate with the cloud based IoT platform.
IoT Platform	System	Facilitates remote control of smart home appliances and facilitates services for the home. This may include home automation management system to the service providers, data storage, data ingestion, high speed distributed big data processing, data analytics, rule engine, alerts configuration, remote commands and application enablement features along with integration capabilities with existing enterprise systems, databases and third-party APIs.
Owner's Smartphones and tablets	Device	Devices using which the owner will monitor and control smart home appliances locally or from remote locations in a secured manner.

Table 8-6 – Actor description

Actor Name	Actor Type	Role Description
Society/Community/City Office	Organization	Township or society office that offers emergency and maintenance services to the residents.
Third Party Services	Organization	Ambulance, fire extinguisher, police, utility companies, etc.
Appliances	Person	Typical home appliances. e.g., electrical appliances (air conditioner, refrigerator, boiler, microwave), lights/tubes/CFL, etc. It may be possible to control/monitor these appliances by connecting them to IoT enabled devices (e.g., A/C connected to a smart switch).
Smart appliances	Person	Off the shelf appliances available in the market. Smart appliances supporting standard protocols may be integrated with the smart home solutions relatively easily.

b. Contextual Illustration

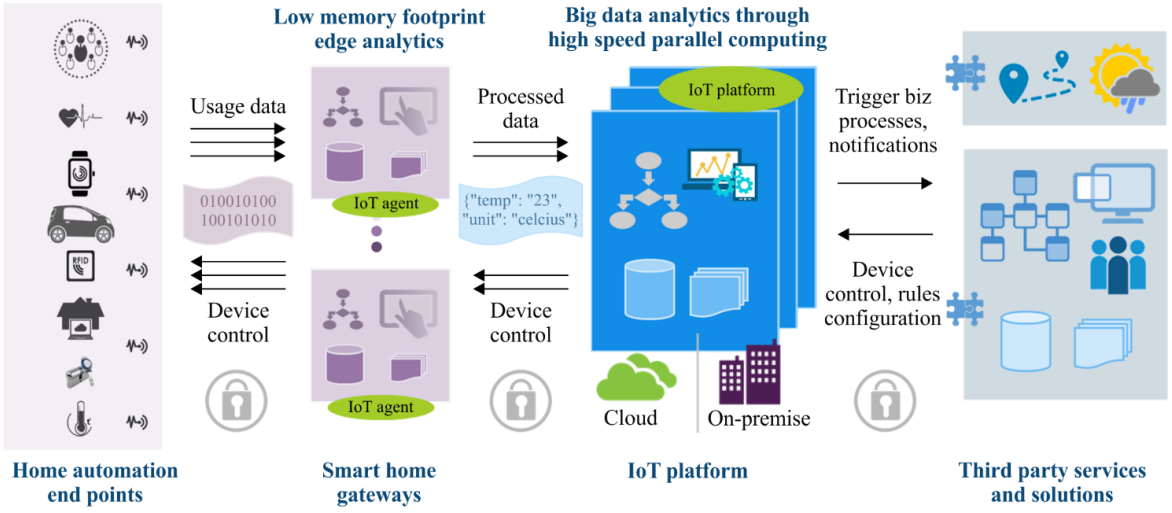


Figure 8-16 – Home automation system contextual description

A highly-available Internet connection is assumed present for the gateway to communicate with stakeholders for them to be able to remotely monitor and control smart home appliances. Alternatively, the gateway is capable of storing the data locally and send it when connectivity is restored.

c. Triggers

- Events occurring inside the home; events can be as simple as switching on a boiler or as critical as smoke detector raising an alarm.
- Control commands invoked by home owners or service providers such as "turning on the AC".

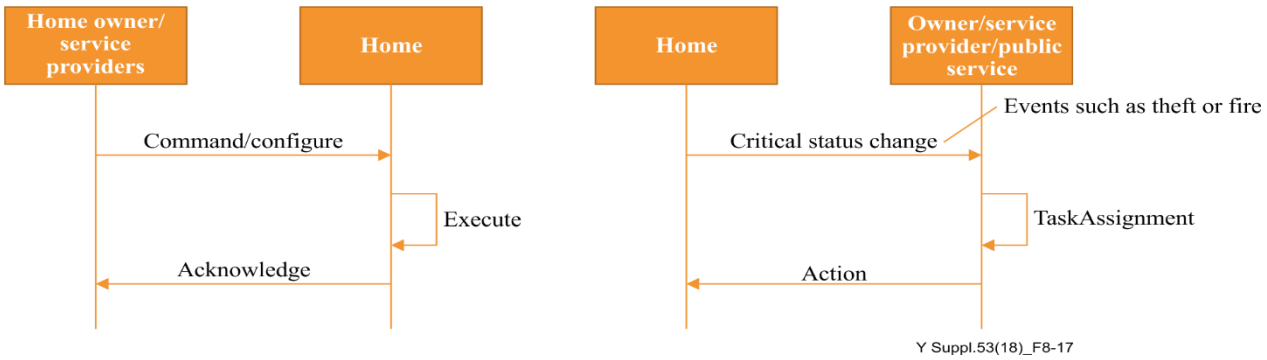


Figure 8-17 – Triggers in home automation system

d. Scenario

- Service provider deploys smart switches, IoT enabled sensors, home monitoring equipment, smart home gateway, etc. and configures the system by registering the gateway and smartphones that are entitled to operate the system and standard rules.
- The home owner can change the configuration as per his preferences and installs smartphone App on the registered phones.
- The gateway controls smart appliances as per the rules in order to save energy or ensure safety.
- The home owner operates smart appliances through the HMI interface provided by the gateway or through smartphone apps.
- The home owner receives usage reports from the system by email.
- The home owner receives push notifications from the system in case of emergency. Notifications are also sent to third party service providers depending on the configuration.
- The home owner can communicate with guests at the door in case the whole family is way.
- Usage and operational data are stored in IoT platform for trending and analysis

e. Process flow diagram

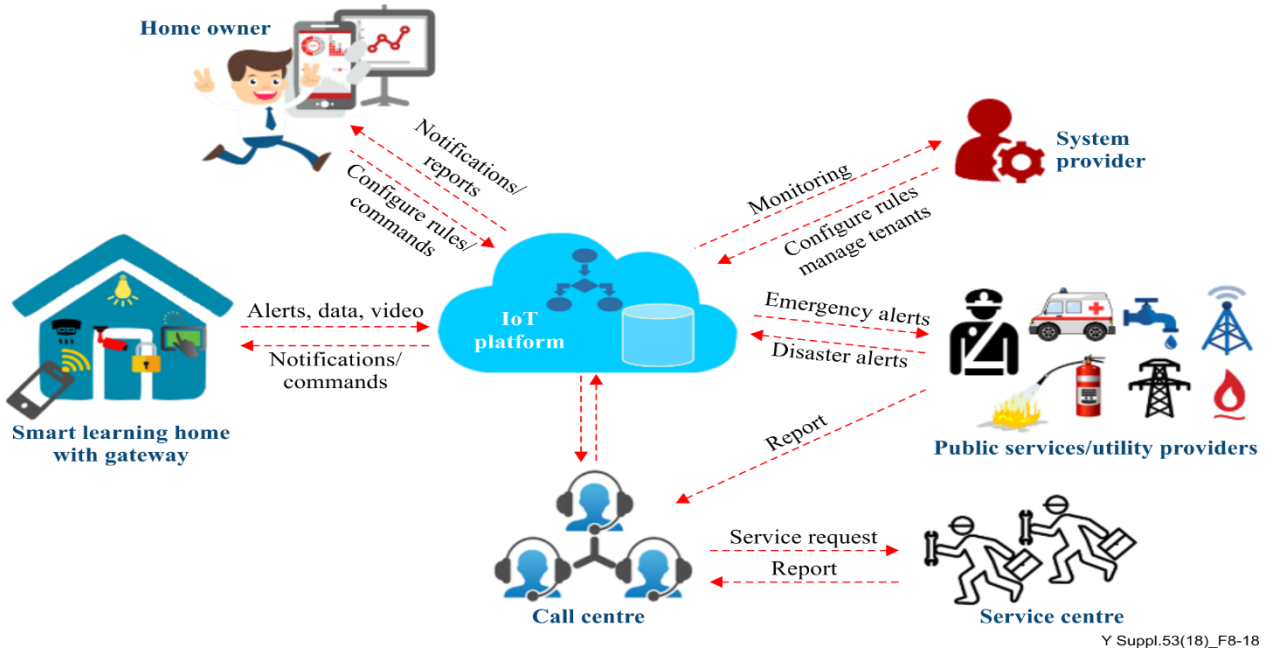


Figure 8-18 – Home automation system process flow

f. Information exchange

From smart devices to gateway:

- device/smart appliance health status;
- device specific data;
- usage history.

From gateway to IoT platform:

- consolidated device/smart appliance health status;
- consolidated device data;
- consolidated usage history;
- rule execution log, alerts log and device control commands log.

From IoT platform to smartphone:

- consolidated device/smart appliance health status;
- consolidated device data;
- consolidated usage history;
- alerts.

From smartphone to IoT platform:

- device control commands;
- rules configuration.

From IoT platform to gateway:

- software updates;
- rules configuration.

From gateway to smart devices:

- health check polling;
- device control commands.

5. Architectural considerations

a. Deployment considerations

The home automation gateway, as well as IoT enabled devices, should be installed inside the house. The location of the gateway should be such that it will ensure uninterrupted Internet connectivity. From the installed location, the gateway should also be able to communicate with IoT devices either through hard-wired connections or industry standard communication mechanisms.

b. Geographical considerations

None

c. Communication infrastructure

Relevant communication infrastructures are given in Table 8-7.

Table 8-7 – Communication infrastructure

	Communication Network	Technologies
Devices to be connected through Gateway	Home area network (HAN)	Short range communication technologies such as BT, BTLE, NFC, WiFi, ZigBee, Zwave, Homeplug etc.
	WAN	GSM 2G, 3G, LTE; Wi Fi, CDMA, Fixed line broadband. Network should have Ipv6 or dual stack (IPv4 and IPv6) capability.
Devices such as Smart meters to be connected directly to the head-end system/Platform	Cellular LPWAN technologies	3GPP Release 13 onwards based technologies, extended coverage – GSM (EC-GSM), narrowband-IoT (NB-IoT) and LTE MTC
	Non-cellular LPWAN technologies	Long-range applications (LoRa), Sigfox etc.

LPWAN technologies have been designed to have long range, consumes very low power and carry very small data.

Devices in the HAN may be connected to the gateways on HAN communication technologies. Gateway may have one or more communication technologies in the HAN/WAN.

The home IoT gateway should support multi-protocol access and interchangeability for working with multiple vendor's devices. It may also have more functionalities such as AI and edge computing to provide alert in case of emergency. Interface is also required at the gateway to make it more interactive for the user through mobile devices, e.g., smart phones/laptop. The home gateway should work as a Smart home control centre.

Not all communication technologies in the HAN may have the capability of IPv4/IPv6. However, it is required that all the devices/gateways (to be connected directly to PSTN/PLMN) should have IPv6 or dual stack (IPv4 and IPv6) capability.

In view of the IAB statement on IPv6 [IAB IPV6], IPv4 support may not be available in future developments, therefore transition to IPv6 only in PSTN/PLMN networks and Gateways / devices to be connected directly to these networks will be required.

d. Performance criteria

The system should be able to raise critical alerts or execute rules in near realtime subject to availability of connectivity.

e. Interface requirements

- Gateway should be able to send alerts/notifications and receive commands using communication technologies mentioned in, but not limited to, "c. Communication Infrastructure" above.
- Smartphones carried by home owners should be able to exchange information with Gateway via IoT platform on wide area network communication technologies.
- Service providers should get alerts on devices running services operated by the Service Providers.
- Service provider should be able to communicate with the home owner for emergency or service calls.
- Protocols used for exchanging messages among different Service providers should ensure scalability and high performance.

NOTE – This may require service providers to adopt SOA [Open Group]/microservices architecture [microservices.io]. For data exchange, existing standards such as representational state transfer (REST), advanced message queuing protocol (AMQP), message queuing telemetry transport (MQTT), refer to [OASIS]. Standard bodies (or consortiums) may standardize the data formats based on ontology.

f. User interface

Web based responsive application should be provided for the service providers to carry out functionalities such as home owner registration, IoT device provisioning, monitoring, etc. Smartphone App should be provided for home owners to perform various activities such as viewing alerts, monitoring/operating smart appliances, etc.

g. APIs to be exposed to the application from platform

The platform should provide REST API for third party service providers' application integration.

h. Data management

Management of data rate, payload size, frequency of communication, synchronous or asynchronous session types, request-, request-acknowledge-, handshake-request-, response types, and broadcast constitute data management requirements in addition to data integrity.

i. Data backup, archiving and recovery

Platform will keep a log of data exchanged between gateway and home owner's smartphone or tablet. Live data will be maintained only for the duration defined in the service level agreement (SLA) between the home owner and the service provider; old data will be purged. The SLA will also guide when backups are performed and data is archived.

j. Remote device management

The approach will allow the home owner to provision, configure, monitor and control smart appliances. Service providers will be able to monitor health of the gateway, IoT enabled devices/sensors and smart appliances.

k. Startup/shutdown process

Startup/shutdown process is specific to gateway, devices and smartphones carried by home owner.

l. Safety and security requirements

Communication between home owner's device and gateway should be encrypted. Gateway as well as smartphones will be authenticated during each transaction with the IoT platform preventing malicious intrusion.

To achieve an appropriate level of safety and device security, as also avoid unwanted vulnerability, devices are required to be tested and certified by a test house certified by the relevant SDO/statutory standardization authority before deployment in the network. Device testing is required against EMC, safety, device security and other Technical requirements related to communication technology and functional capabilities (e.g., SAR, IPv6).

6. Potential market growth forecast

Global scenario: Smart and connected home market is increasing rapidly across the globe. According to one forecast, home automation market is expected to reach US$ 79.5 billion by 2022, at a CAGR of 11.3% [MarketsandMarkets].

According to another research, by 2020 more than 40% of Indian urban households will use home automation or energy management solutions [Gartner]. Homes will move from being

interconnected to becoming information- and smart-enabled, with an integrated services environment that not only provides value to the home, but also creates individual-driven ambience. The home will become the personal space that provides assistance or personal concierge experiences to the individual as per Gartner report [Gartner].

7. Implementation constraints

Some of the challenges anticipated are as follows:

- Lack of high-speed reliable network coverage;
- Interoperability between disparate network technologies;
- False emergency alarms detection;
- Replacement of batteries in IoT enabled devices or smart appliances, if any;
- Personally identifiable information concerns of consumers.

8. Available global standards

Standard No.	Title
TS 103 267 v1.1.1 (2015-12)	SmartM2M; Smart Appliances; Communication Framework, ETSI
TS 103 264 v1.1.1 (2015-11)	SmartM2M; Smart Appliances; Reference Ontology and oneM2M Mapping, ETSI
CTC/TC 205	Home and Building Electronic Systems, CENELEC
ETSI TS 103 424 V1.1.1 (2016-11)	Smart Home architecture and system requirements
ETSI TS 103 425 V1.1.1 (2016-11)	Wireless HANs
ETSI TS 103 426 V1.1.1 (2016-11)	Requirements For HGI Open Platform 2.1

8.6 Advanced metering infrastructure

1. Title of the use case

   a. Name of the use case: advanced metering infrastructure (AMI)

   b. ID of the use case: smart metering/001/17-18

   c. Version/revision history: 001/Dec/2018

   d. Source: India/MoC/TEC

2. Objective of the use case

AMI is a system which typically includes smart meters, communication infrastructure, data concentrators or gateways, head-end system (HES) and a meter data management system (MDMS) and integration with existing IT applications such as enterprise resource planning (ERP), metering, billing, collection (MBC), geographical information system (GIS), outage management system (OMS), customer portal, advanced analytics etc. The following functionalities can be achieved:

   a. Scheduled and on-demand meter data collection

   b. Remote firmware upgrade

   c. Clock synchronization

   d. First breathe and last gasp notifications to the HES

   e. Remote connect/disconnect on the following conditions

      i. non-payment of bill, customer request

ii. over current

iii. load control limit

iv. Pre-programmed tamper conditions

v. disconnect signal from utility control centre

vii. in case of prepaid facility under defined/agreed conditions

f. Event logging (including tampers)

g. Cry-out alarms in case of critical events

h. Basic power quality parameters

i. Remote meter configuration such as maximum demand threshold, tariff tables, disconnection threshold for load control or updating meter's balance in case of pre-paid metering

3. Background

a. Current practice

Meter readers acquire meter-reading data manually either by visual reading or through spot meter reading using handheld devices. This reading data is uploaded to the billing system of the utility at the end of the day or later. Meter readers follow a meter reading route sequence to cover the meters in an area. This often results in missed readings (due to meter premises locked or other reasons), wrong readings (visual reading error), missed consumers (meter not listed in the reading list) etc. Errors creep in during the uploading process (incorrect manual upload, validation failures etc.). The entire process is time consuming.

Apart from the errors in the billing readings as described above, there is no information on the consumption pattern of individual consumer at a granularity less than the billing period. In addition, the quality of supply to the end consumer cannot be monitored and the tampers or faults in meter go unnoticed.

Utilities have already established meter reading systems that use handheld units for meter data acquisition of their 'high revenue' consumers. Meters have been installed at distribution transformers for monitoring the aggregated energy consumption of downstream consumers.

b. Need for use case

With the advent of an AMI, both consumers and the utilities would benefit. The consumers would be able to:

- View their consumption of electricity accurately on a regular basis.
- Manage loads in different manners based on the design, ranging from remotely turn ON/OFF their appliances to managing total demand to allow curtailed supply instead of load-shedding.
- Save money from time of use (ToU) tariffs by shifting non-priority loads.
- Face reduced outages and downtimes, and even lower or zero load-shedding.

Utilities benefit in the following ways (and of which are passed on to consumers):

- Financial gains by:

i. managing the load curve by introducing ToU/time of day (ToD) tariff, demand response etc.

ii. reducing equipment failure rates and maintenance costs

iii. enabling faster restoration of electricity service after fault/events

iv. detecting energy theft/pilferage on near real-time basis

v. streamlining the billing process

vi. remote meter reading which reduces human resources, human errors and time consumption for meter reads

- Respond to power outages and detect meter failures (with no on-site meter reading).
- Enhanced monitoring of the system resources that would significantly improve the reliability.
- Improvement in other key performance indicators.

c. Indian ecosystem specifics

The Indian utilities, regulators, policy makers are aware about the potential of AMI as the foundation for not only smart grids, but also to improve their operations in a business as usual scenario to serve their consumers.

Automatic meter reading (AMR) has been implemented in more than 50 utilities in 1400 towns across the country, covering on an average 50000 meters per utility, under the restructured accelerated power development and reforms programme (R-APDRP) scheme alone. This program is being extended to cover other parts of the country under the integrated power development scheme (IPDS).

India's smart grid vision is to 'transform the Indian power sector into a secure, adaptive, sustainable and digitally enabled ecosystem that provides reliable and quality energy for all with active participation of all stakeholders.' Smart grid technology pilots are being implemented in a few utilities to gain experience as a pre-cursor to a full rollout. The primary focus of these pilots is AMI and peak load management.

4. Description

a. Ecosystem description in terms of actors and business roles

Table 8-8 depicts the various actors in AMI and their description:

Table 8-8 – Actors in AMI

Actor Name	Actor Type (person, organization, device, system)	Role Description
Smart Meter	Device	The meter is the device that measures and stores the electricity parameters of interest.
Communication Infrastructure	System	The communication infrastructure is the system that facilitates the data exchange between meter and Back-end Systems. Such as gateways, DCU, nodes etc.
Head-end system	System	HES is the system to collect the meter data and manage network and smart meter operations.
AMI Configurator	Person/system	Configures type of data to be acquired, periodicity of its acquisition and list of meters from which to acquire.
AMI administrator	Person/system	Monitors the AMI process for error free operations.
Consumer	Person	Consumer of electricity.
Utility Staff	Person	Utility staff are users of the AMI system with predefined roles and access privileges.

Table 8-8 – Actors in AMI

Actor Name	Actor Type (person, organization, device, system)	Role Description
Meter Data Management System	System	MDM is the repository of meter readings. It validates data arriving from AMI for completeness and accuracy. If data for some intervals has not arrived from a meter, MDM flags this to the AMI Administrator or requests the AMI to re-acquire this data on-demand.

b. Contextual Illustration

A smart meter can be connected to the HES directly on wide area network communication technologies or through a gateway/data concentrator unit (DCU). The contextual illustration of AMI is depicted in Figure 8-19.

Details of various communication technologies in the field area network (FAN)/neighborhood area network (NAN) and wide area network have been described in Table 8-9 in this clause in 5c.

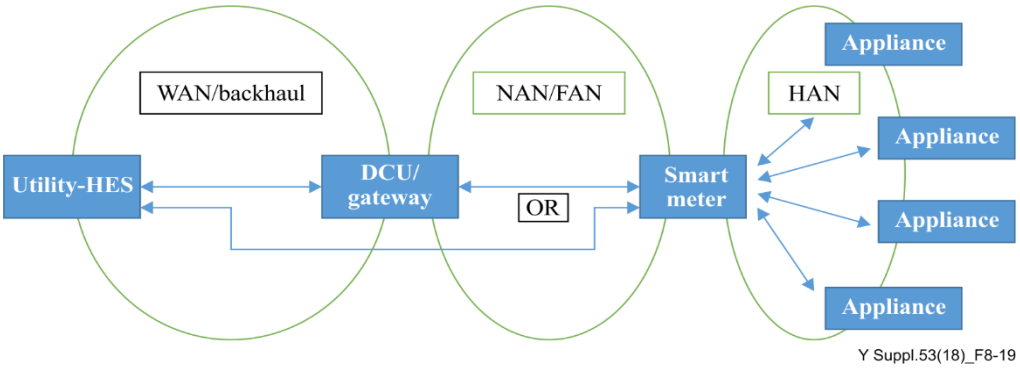


Figure 8-19 – Contextual illustration of AMI

There are multiple scenarios of AMI use case as mentioned below:

- Scenario #1: remote meter registration;
- Scenario #2: remote meter configuration;
- Scenario #3: scheduled meter reading;
- Scenario #4: on-demand meter reading;
- Scenario #5: event notification and cry-out alarms;
- Scenario #6: communicate with consumer over AMI through in-home display (IHD)/consumer portal;
- Scenario #7: remote meter operation;
- Scenario #8: remote over the air programming;
- Scenario #9: remote meter power supply status;
- Scenario #10: remote meter health monitoring;
- Scenario #11: remote meter time synchronization.

c. Pre-requisite

The smart meter is installed in the field with an activated communication module. AMI HES and gateway (if applicable) are available. End to end network connectivity is in place for remote communication.

d. Precondition

Smart meter details are available in the AMI head-end master. Back-end systems are integrated.

e. Triggers

- new smart meter is installed in the field and powered up for registration;
- the HES triggers requests for on-demand data read, remote configuration, firmware upgrade, time synchronization;
- smart meter triggers for schedule meter reading, event notification (occurrence of an event), communication with IHD, power supply status, meter health parameters;
- connect/disconnect:
  i. user-triggered: utility authorized person responds to consumer request for temporary disconnection or for disconnecting supply to consumers found tampering etc.;
  ii. utility revenue system: remote disconnection due to non-payment of dues or reconnection after pending dues have been cleared;
  iii. prepayment system initiated on breaching minimum credit balance limits;
  iv. HES for remote load control.

f. Description

- installation of the smart meter and its commissioning with the HES.
- periodic data and on-demand data collection from the smart meters by HES using communication network.
- critical events, alarms and outage detection communicated to the utility back office upon its occurrence.
- consumer load disconnection / reconnection remotely.
- remote configuration and FOTA of smart meters.
- AMI system is used to monitor operating condition of the meter remotely at granular intervals and compare with the standard conditions of equipment.

In detail:

The smart meter connects to the HES directly or through gateway, the first time, and provides its details (name/serial no., unique identifier and address). The AMI system verifies with the HES that this meter is authentic. The HES initiates all configurations. The AMI system is configured for meter reading, remote operations etc. Critical events are configured to be notified to the HES immediately on detection. Normal priority events are notified to the HES at a scheduled frequency and/or when the total number of events exceeds a threshold number. The smart meter clock is synchronized with the system reference clock.

The smart meter data acquisition is initiated by the smart meter (push data) as per schedule configured in the meter. Data from the smart meter can be polled on demand from the HES (pull mode) whenever triggered in the HES automatically or by the AMI administrator.

Data and events generated in the AMI system can be further propagated to a meter data management system for processing, collation and analytics as well as for further routing to other utility systems.

Consumer load disconnection and reconnection can be done locally by the meter itself or command from the utility systems. The smart meter validates the request by authenticating the requestor credentials. The smart meter can send an acknowledgement for receipt of command request to the initiator. Remote switching operations of the smart meter is communicated to the consumer via email or short message service (SMS) as well as published to the utility portal as a notification for the consumer.

For smart meter firmware upgrades, the firmware version of the smart meter (destination device) is compared with the 'target' firmware version. If the smart meter version is lower, the HES initiates a transfer of the higher version firmware to the smart meter. Once the transfer is completed, the smart meter switches to the higher version firmware. After switching onto the higher version, the smart meter reports its new version to the HES. If the firmware download is interrupted due to a power failure or break in the communication link, the HES and smart meter will terminate the download session. The HES will then have to re-initiate the download activity when acceptable conditions restored.

g. Post-conditions

- smart meter registration and commissioning is completed in the AMI system.
- smart meter data is made available in the back-office systems for use.
- various reports are generated and decisions are made based on the reports.
- manage and maintain the AMI system on regular basis.

In detail:

A valid meter is registered in the system and the smart meter is activated. Initial smart meter readings and date of activation of the smart meter at the current location are recorded in the system. Data are made available to the head-end, MDMS and utility systems at scheduled intervals. Reports, error alerts and logs are provided to the AMI system administrator. If required, the firmware version in the smart meter is upgraded and smart meter is able to resume operations once the new firmware version is successfully installed.

h. Information exchange

Information exchanged includes smart meter details for meter registration, meter parameters configuration details, messages and time of configuration, meter data for reading, meter firmware for remote firmware upgrade, control commands for meter operation, notifications such as power supply status, alarms, and health messages from meter to HES etc. Information is exchanged with bidirectional flow of data in real-time; high confidentiality, integrity and availability requirements apply.

i. Process Flow Diagram

The smart meter registration process begins as soon as the meter is deployed in the field. The smart meter sends information such as meter serial number, communications identifier and keys to the HES. The smart meter sends periodic data (register, interval) to the HES. The HES sends commands to the smart meter for on-demand meter data reading, either scheduled or triggered by the head-end user.

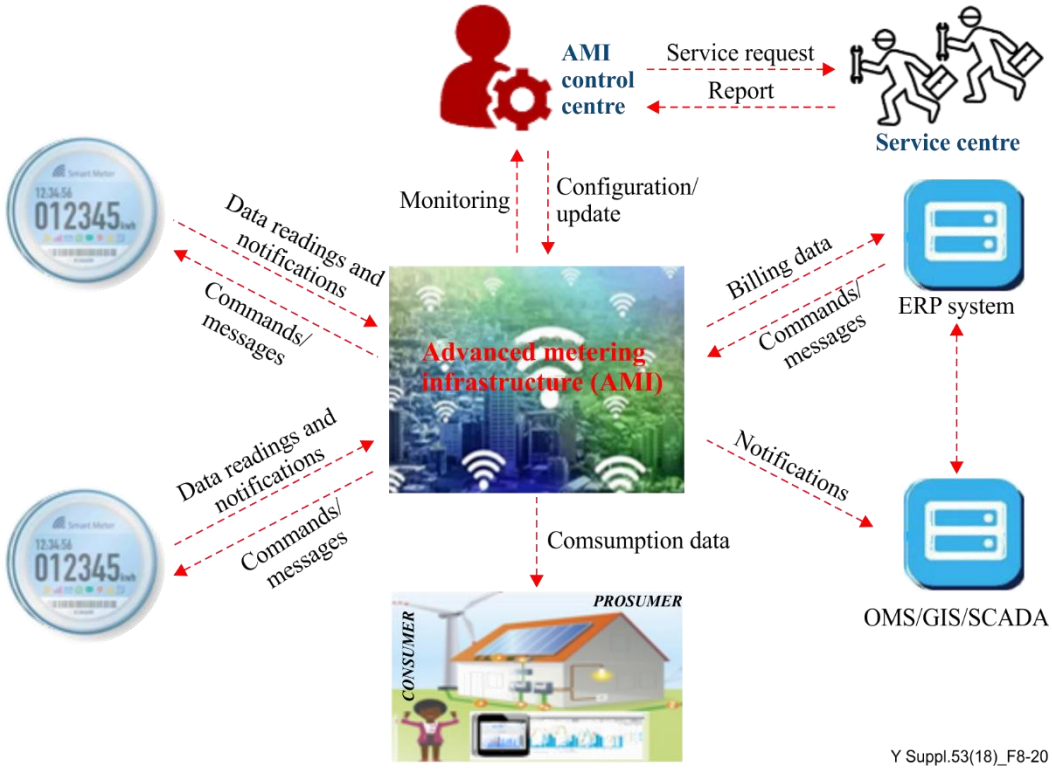


Figure 8-20 – Process flow diagram

5. Architectural considerations

a. Deployment considerations

Smart meters are installed at consumer premises can be prone to electrical noise interference. The installation of DCUs may not have reliable power supply, and hence battery powering maybe required.

The DCU/gateway is installed at a location where cellular network (3G/4G) coverage and signal strength for back-haul connectivity is available. The communication network and its architecture is deployed across a distribution area to enable applications such as street lighting, sensors, distribution automation etc., in addition to smart metering.

Smart meters enabled with communication capabilities connect to a DCU/gateway and then to the HES.

b. Geographical Consideration

Meters are widely dispersed or installed in clusters. DCUs/gateways are widely dispersed.

c. Communication Infrastructure

The communication network can be deployed by the utility or be made available via a third party in the metering area. Table 8-9 describes available technologies used for AMI.

Table 8-9 – Communication technologies used for AMI

Sl. no./scenario	Communication network	Related technologies
Devices/smart meters connected directly to head-end system.	Smart meters connected on wide area network technologies to PSTN/PLMN.	GSM 2G, 3G, LTE, CDMA, EC-GSM, NB-LTE/NB-IOT, LTE Cat-M1. Devices, as well as networks, should have IPv6 or dual-stack (IPv4 and IPv6) capability.
Devices/smart meters connected through gateway/DCU to head-end system.	Smart meters connected on short range communication technology to gateway in field area network (FAN)/neighbourhood area network (NAN).	• RF mesh network: 6LoWPAN, ZigBee etc. • (PLC): Prime PLC, G3-PLC etc.RF star network: LPWAN non-cellular technologies – LoRa, Sigfox etc.
	Gateway/DCU connected to HES on WAN technologies.	GSM 2G, 3G, LTE; WiFi, CDMA, Fixed line broadband, Ethernet. Gateway as well as Network should have IPv6 or dual stack (IPv4 and IPv6) capability.

- interoperability and open standards: integrate any smart meter by way of open standards into network;
- lightweight: limited resources in terms of power, CPU, memory, and storage;
- versatile: IP architecture is well equipped to cope with any type of physical and data link layers, making it future proof as various media can be used in a deployment and, over time, without changing the whole solution architecture and data flow;
- scalable: massively deployed and tested for robust scalability;
- manageable and secure: communication infrastructure requires appropriate management and security capabilities for proper operations;
- reliability: successful number of attempts to get the data or complete the transactions like remote connect/disconnect, TOU settings, time sync etc.;
- ability to meet present and future business needs and use cases.

Not all the communication technologies in the HAN may have the capability of IPv4/IPv6. However, it is required that all the devices/gateways (to be connected directly to PSTN / PLMN) have IPv6 or dual stack (IPv4 and IPv6) capability.

In view of the IAB statement on IPv6 [IAB IPV6], IPv4 support may not be available in future developments, therefore transition to IPv6 only in PSTN/ PLMN networks and Gateways / devices to be connected directly to these networks will be required.

d. Performance criteria

For seamless operation of AMI, reliability, latency, network security and total cost of ownership of the communication technologies are key.

Data availability from smart meters is key to meeting all business scenarios. Performance criteria are defined in a service level agreement (SLA) which includes meter data availability, successful metering operations, remote manageability, network availability and reliability, and applications availability.

e. Interface requirements

Figure 8-21illustrastes key interface requirements.

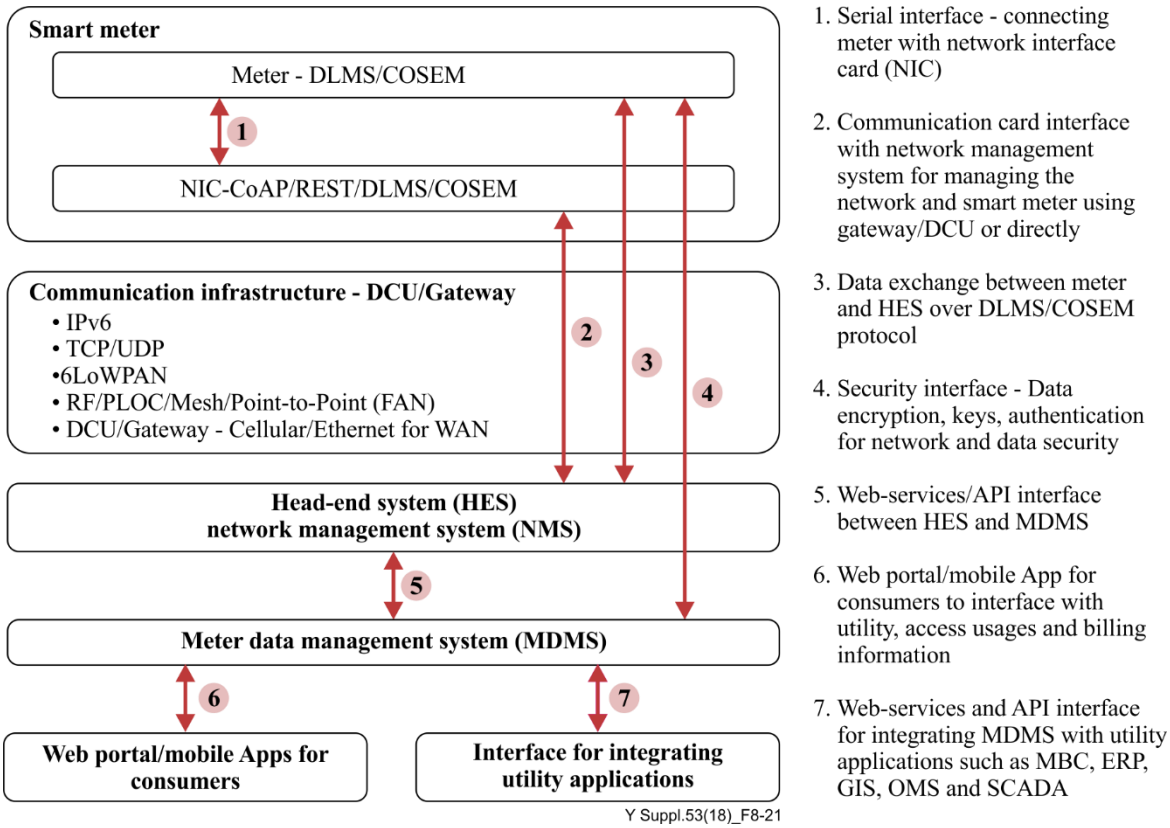


Figure 8-21 – Interface diagram

f. User interface

The web user interface of the HES and network management system is available for authorized users for device management, configuration, and firmware upgrade and troubleshooting end devices (smart meters) and network components (DCU/gateways, routers etc.).

g. APIs to be exposed to the application from platform

The following APIs exposed from the platform to the application:

- APIs for monitoring and managing the NAN and WAN segments of AMI;
- APIs for a network management system (NMS) – required for connectivity and desired data throughputs;
- APIs for tracking location of meters and gateway;
- APIs for configuring data transfer priority.

h. Data Management

The MDMS and an NSM are responsible for data management and network management respectively. Smart meter data is managed in the MDMS; this supports storage, archiving, retrieval and analysis.

i. Data backup and archiving

The smart meter stores interval data and billing data for periods of more than a month. The HES should support the storage of raw smart meter data, alarms and alerts for a minimum of three days to 90 days, depending upon project and information security requirements. Data backup and archiving should be done weekly and monthly. This should support incremental data backup, files backup etc. Gateway data backup can be taken remotely. The DCU should have storage capabilities.

j. Remote device management

Remote devices should support the required protocols for remote manageability of the devices such as over the air firmware upgrade and remote configuration etc.

k. Startup/shutdown process

The smart meter will register itself with the HES on each power-cycling event (i.e. a normal power-on event that can be hardwired or a soft power-cycling event). DCU/gateway power cycling or restart will also trigger relevant smart meters to re-register with it. It is expected that the HES is operational prior to the DCU/gateway being operational. DCU/gateway is expected to be operational before related smart meters.

l. Safety and security

Smart meters (devices), DCUs, gateways etc. need to be protected from vulnerabilities and hacking. Regarding information security, smart meter data needs to be confidential, and integrity and non-repudiation must be maintained. In addition, denial of service attacks must be prevented. Smart meters should be tested and certified by technical organizations for EMI/EMC, safety, device security, communication technologies related parameters, IPv6, restriction of hazardous substances (RoHS), etc.

The system should manage security keys and certificates, and should report any security breach or unauthorized communications logged by devices. The system should have audit trail functionality for managing and storing all the records of activities performed by the users. All data exchange at every step should be encrypted using advanced algorithms and keys.

6. Potential market growth

In India, a number of smart metering pilot projects and also the deployments are in progress. India has launched several initiatives, including Smart Cities, and released government policies that stress the need for building smart grids. Under Ujwal DISCOM Assurance Yojana (UDAY) program Government has targeted to to deploy 35 million smart meters by December 2019. Energy Efficiency services Limited (EESL) is deploying smart meters through Smart Meters National programme (SMNP) and has a target to replace 250 million conventional meters with the smart meters [Indian Infra Pub].

7. Challenges

The following are the challenges for AMI rollout in India:

- limitations in various last mile connectivity solutions;
- end-to-end interoperability standards to integrate AMI systems;
- system security – need standards and regulations;
- latency in the reception of signals;
- coverage of the communications network not 100%;
- industry readiness for manufacturing of smart meters;
- utilities lack clarity on functional requirements and business models;
- system security concerns especially balancing firmware upgradability with usability;
- manpower limitations for deployment, usage and management – both in the power distribution companies (DISCOMs) as well as in the industry.

8. Contracts and regulations

All smart meters installed in India must follow central electric authority (CEA) regulations regarding installation and operation of smart meters. In addition, all communicating devices must follow standards set by wireless planning and coordination (WPC) regarding frequency bands, channel bandwidth, transmitted power etc.

9. Available global standards

Table 8-10 list global standards on energy metering.

Table 8-10 – Global standards on energy metering

Standard Number	Title
International Electrotechnical Commission (IEC) 62056	Set of Standards for Electricity metering data exchange. Adopted by India as IS15959
IEC 62056 / EN 61036	Alternating current static watt-hour meters for active energy (classes 1 and 2). Adopted by India as IS13779
IEEE 802.15.4	Standard for local and metropolitan area networks
IEEE 1901.2	Standard for low-frequency narrow band power line communications
IS 16444	Indian Smart Meter standard
IS 15959-2	Performance levels for collection of daily meter readings
EN 13757-1	Communication systems for meters and remote reading of meters – Part 1: Data exchange
EN 62056-1-0	Electricity metering data exchange – The device language message specifications (DLMS)/COSEM suite – Part 1-0: Framework
ETSI TS 102 221	Smart Cards; UICC Terminal interface; Physical and logical characteristics
ETSI TS 102 223	Smart Cards; Card Application Toolkit (CAT)
ETSI TS 102 671	Smartcards, ; Machine to Machine UICC; Physical and logical characteristics
ETSI TS 102 225	Smart Cards; Secured packet structure for UICC based applications
ETSI TS 102 484:	Smart Cards; Secure channel between a UICC and an end-point terminal.
ETSI TR 102 691	Technical Report – M2M Smart Metering Use Cases
CEN/CLC/ETSI/TR 50572:2011	Functional reference architecture for communications in smart metering systems
IEC 62052-11 / CISPR 11	Conducted Emission & Radiated Emission or Disturbance Voltage disturbance (150kHz-30MHz)
IEC 61000-4-6	Immunity to Conducted Susceptibility (80MHz-2GHz) with 10V/m
IEC 61000-4-4	Electric Fast Transient Burst Test
IEC 61000-4-2	Electro Static Discharge Test
IEC 61000-4-5	High Energy Surge Immunity Test
ETSI TR 50572	Functional reference architecture for communications in smart metering systems

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2019