सत्यमेव जयते

TECHNICAL REPORT

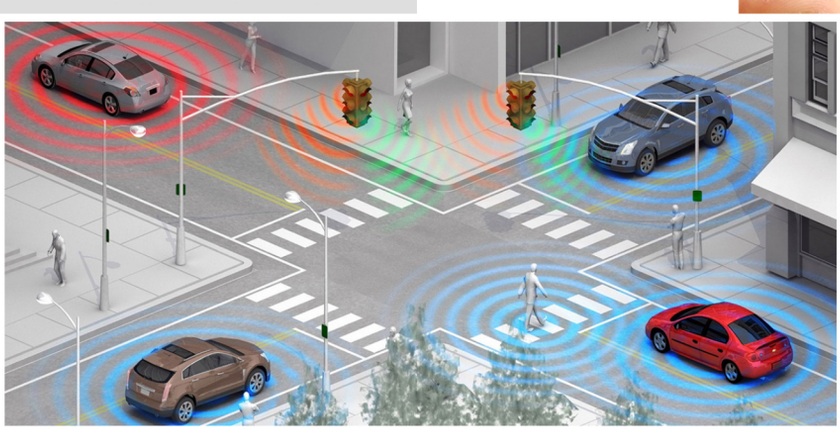
M2M ENABLEMENT IN

INTELLIGENT TRANSPORT SYSTEMS

V2V/ V2I RADIO COMMUNICATION AND EMBEDDED SIM

TEC-TR-S&D-M2M-003-02

M2M AUTOMOTIVE WORKING GROUP



ISO 9001:2008

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

RELEASE 2.0

NOVEMBER 2015

सत्यमेव जयते

TECHNICAL REPORT

M2M ENABLEMENT IN

INTELLIGENT TRANSPORT SYSTEMS

V2V/ V2I RADIO COMMUNICATION AND EMBEDDED SIM

TEC-TR-S&D-M2M-003-02

M2M AUTOMOTIVE WORKING GROUP

ISO 9001:2008

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

RELEASE 2.0

NOVEMBER 2015

Revision History

Date	Release	Document No.	Description
20/11/2015	R2.0	TR-S&D-M2M-003-02	V2V / V2I radio communication and embedded SIM

Important Notice

Individual copies of the present document can be downloaded from http://www.tec.gov.in
Users of the present document should be aware that the document may be subject to revision or change of status.
If you find errors in the present document, please send your comment to dirsd1.tec@gov.in.

Disclaimer

This document is meant for circulation amongst all the stakeholders in the field of M2M/ IoT/ ICT. The information contained is mostly compiled from different sources and no claim is being made for being original. Every care has been taken to provide the correct and up to date information along with references thereof. However, neither TEC nor the authors shall be liable for any loss or damage whatsoever, including incidental or consequential loss or damage, arising out of, or in connection with any use of or reliance on the information in this document. In case of any doubt or query, readers are requested to refer to the detailed relevant documents.

Table of Contents

Figures

Tables

List of Contributors

A. Joint Working Group (JWG) Chairman:

Name	Designation	Organisation	Email Address
A. K. Mittal	Sr. DDG	Telecommunication Engineering Centre (TEC)	srddg.tec@gov.in

B. Joint Working Group (JWG) Secretariat:

Name	Designation	Organisation	Email Address
Sushil Kumar	DDG	Telecommunication Engineering Centre (TEC)	ddgsd.tec@gov.in

C. Working Group (WG) Chairs:

	Name	Designation	Organisation	Email Address
Chairman	Anuj Ashokan	Lead IoT Solutions	Tata Teleservices Ltd.	anuj.ashokan@tatatel.co.in
Rapporteur	Alok Sethi	DGM (TTS)	DIMTS	alok.sethi@dimts.in
Co-Rapporteur	Rajeev Kumar Tyagi	Director (S & D)	Telecom Engineering Centre	dirsd1.tec@gov.in

D. Primary Authors:

S.No.	Name	Organisation	Email Id
1.	Vikas Phogat	Morpho	vikas.phogat@morpho.com
2.	Alok Sethi	DIMTS	alok.sethi@dimts.in
3.	Sharad Arora	Sensorise Digital Services Pvt Ltd	Sharad.arora@sensorise.net

E. Contributors:

Name	Organisation	Name	Organisation	Name	Organisation
Abhishek Srivastava	DIMTS	Alok Sethi	DIMTS	Abhash Sharma	DIMTS
Mr TP Malik	idiagnosis	Dinesh Chand Sharma	ETSI	Abhijit Mulay	ARARI
Sushil Kumar	TEC	RaunaqueQuaiser	STMicroelectronics	Anuj Ashokan	Tata Teleservices Ltd
Rajeev Kumar Tyagi	TEC	Anupam Vibhuti	Worxpace CPL	Kishor narang	Narnix Techno Labs
Shirsanka Saha	Tata Teleservices Ltd	Shivalik / Rishi kalra	Mapmyindia		

F. Editorial Team:

S.No.	Name	Organization
1	A K Mittal	TEC
2	Sushil Kumar	TEC
4	Anuj Ashokan	TTSL
6	Alok Sethi	DIMTS
10	Sharad Arora	Sensorise Digital Services Pvt Ltd
11	Rajeev Kumar Tyagi	TEC

Executive Summary

In the Release 1 of the Technical Report on M2M enablement in ITS, it was noted that with a robust IT and telecom infrastructure in place, India stands to gain from the use of ITS to alleviate urban transport issues. Use of such technologies can be vehicular or infrastructural. As the Indian economy progresses and urbanization in India increases, use of ITS and its importance will increase proportionately. The unique ecosystem and diverse challenges creates plenty of room for R&D for creation of suitable technologies in India.

The 2nd Release takes forward the two major work areas which were identified in Release 1 i.e. V2X communication and ESIM for connected cars.

As part of ITS ecosystem, every vehicle has to communicate with, other vehicles, road infrastructure, people and environment. Wireless communications technology plays a major role in such communication. The report talks about the unique challenges and ecosystem of India along with candidate technologies such as DSRC and LTE etc. for V2X.It also recommends the best way forwards for India in the adaption of technology and meeting spectrum requirement.

The report deals in depth with the requirements of eSIM especially for the automotive sector. It covers, inter alia the following:

a. Standard specification for M2M SIM cards
b. Management of aftermarket device provisioning
c. KYC norms for SIM that can be used in the automotive industry

In addition to the above, the report highlighted the need for standards and guidelines for Emergency Call, or more popularly, E-Call.

The need for review of existing policies on KYC, multiple subscriptions on the same eSIM and security requirements has been highlighted. It has also been recommended that TEC specifications for eUICC may be amended to include the requirements of automotive sector.

1 Background

The first technical Report of the M2M Automotive Working Group was released along with four other reports on Remote Health Management, Intelligent Transport System, Safety & Surveillance and Gateway & Architecture, and the National Telecom M2M Roadmap by the Ministry of Communications and Information technology. The Technical Reports are available at www.tec.gov.in/technical-report/ and M2M Roadmap is available at www.dot.gov.in/ntcell.

The aim of the four sectoral reports was to examine the M2M Applications prevalent in the concerned sector, carry out gap analysis and identify further action points.

The Report on M2M Enablement in Intelligent Transport Systems provided detailed information compiled in to chapters, namely, Need of M2M Communications in the Transport Sector, Conceptual Description of M2M Communications in ITS, Use cases, ITS initiatives in India, Communication Technologies and Standards, Key Challenges and Way Forward.

The earlier reports identified several areas for further work items. This Release addresses two such priority work items, namely:

- V2V & V2I communication technologies and
- Leveraging the Embedded SIM for M2M proliferation

2 Scope

This Release covers broadly the following:.

- Requirements for V2X communication.
- Candidate technologies and roadmap for V2X.
- Recommendations for Indian ITS sector.
- Requirements for eUICC and Remote Subscription Management
- Standards governing the eUICC and Remote Subscription Management
- Policies to proliferate the M2M / IoT Use Cases with the eUICC and Remote Subscription Management

3 V2X Communications

3.1 Indian ecosystem and its requirements

India is a huge market by itself with close to 200 million fleets on road and with a road Infrastructure of 4.2 million kilometres of road. About 90% commuters use road as primary mode of transportation, which make Indian ITS a huge market in itself, however it also comes with some extremely complex ecosystem and its implications on technology can be understood by experience only.

India is a combination of extremely diverse landscape, with Himalaya's ranges and its foothills, Thar Desert, tropical rain forests, plains of central India, long costal belt with western ranges of Sahyadaris and remote rural locations with heavily populated fast growing cities. There are no lane to 8 lanes super highways, which makes it a blue print with almost all type of conditions and challenges. Indian roads also host heterogeneous type of vehicles with two wheelers and pedestrians forming the major part of the ecosystem.

Some requirements of ITS ecosystem are spectrum, mobility with low latency and low bandwidths, extremely high capacity mesh network, stationary high bandwidth with precision of location identification etc. Also with vision of creating future Smart city models with 100 Smart Cities, ITS infrastructure shall also has to part of the larger ecosystem of network for Cities.

3.2 What is V2X Communication

ITS enables elements within the transport system such as commuters, vehicles, roads, traffic lights, message signs to become intelligent, embedding them with microchips and sensors, empowering them to communicate with each other.

Wireless data communication between vehicles is one the technologies which has improved the deployment of the ITS applications. This communication is divided generally into three types.

- Vehicle to Vehicle (V2V) :Vehicles communicates directly with neighbour vehicles

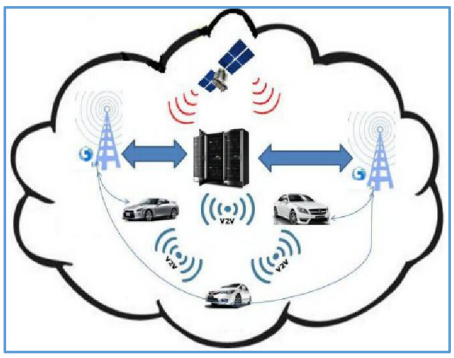


FIGURE 1 ITS COMMUNICATION

- Vehicle to Infrastructure (V2I): Two vehicles communicates indirectly by third party medium (e.g. roadside equipment)
- Vehicle to Pedestrian (V2P): Information exchange between vehicle and pedestrian.

V2X comprises of V2V, V2I and V2P. In this document, V2V and V2I will be discussed.V2X communication is the passing of information from a vehicle to any entity that may affect the vehicle, and vice versa. This information exchange can be used for a host of safety, mobility and environmental applications to include driver assistance and vehicle safety , speed adaptation and warning, emergency response, safety, traveller information, navigation, traffic operations and demand management, personal navigation, commercial fleet planning and payment transactions. There is significant societal benefit and commercial value to delivering safety, mobility and convenience applications that rely on V2X.

3.2.1 Vehicle to Vehicle Communication

Vehicle-to-vehicle communication (V2V communication) is the wireless transmission of data between motor vehicles. The goal of V2V communication is to prevent accidents by allowing vehicles in transit to send position, speed data and panic information to one another over an ad hoc mesh network. Depending upon how the technology is implemented, the vehicle's driver may simply receive a warning should there be a risk of an accident or the vehicle itself may take pre-emptive actions such as braking to slow down.

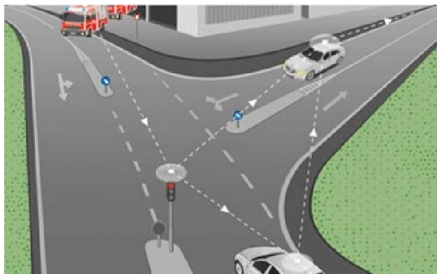


FIGURE 2 V2V COMMUNICATION

The implementation of V2V communication currently has three major roadblocks:

1. Disintegrated ecosystem: Auto OEMs, technology companies, relevant departments transport and highways, Ministry of Home affairs, urban development and ICT department all working together for common standards.
2. Huge base of existing vehicles and uncoordinated deployments.
3. Data privacy concerns and policy adaptation.

3.2.2 Vehicle to Infrastructure Communication

Vehicle-to-Infrastructure (V2I) Communications for Safety is the wireless exchange of critical safety and operational data between vehicles and roadway infrastructure, intended to avoid motor vehicle crashes, optimize traffic, exchange content, enforce pollution norms.

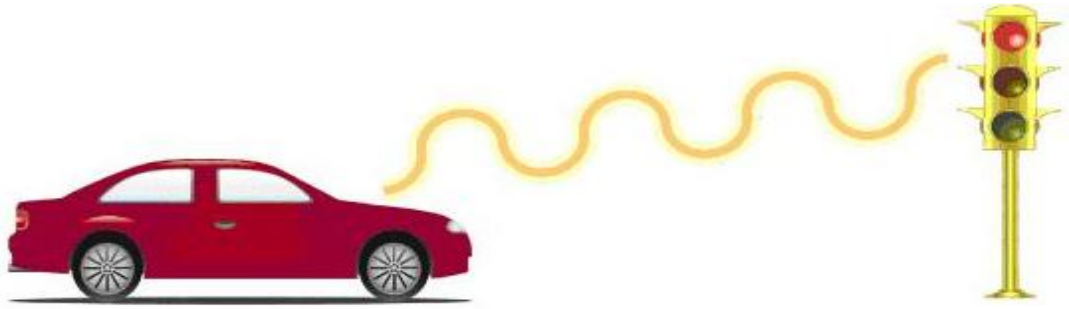


FIGURE 3 V2I COMMUNICATION

V2I applications include Red Light Violation Warning, Curve Speed Warning, pollution under control check etc. The utility of V2I also to enables safety applications designed to avoid or mitigate vehicle crashes, particularly for crash scenarios not addressed by V2V communications alone.

3.2.3 Vehicle to Pedestrian communication

Vehicle to pedestrian communication is required to alert pedestrian of any possibility of an accident. With V2V technology, pedestrians can carry devices (such as mobile phones) that can send out a safety signal using V2X technologies and communicate with V2X devices that would be used in vehicles.

3.3 Services from V2V and V2I

Main uses of V2V and V2I communication services are to transmit information for:

- Roadside beacons
- Traffic signals/controls
- Toll collections
- Petrol pumps and charging centres (for electric vehicles)
- Digital signage
- Safety Applications such as red light violations, overloading or crossing speed limits
- eCall (911 in USA and 112 in Europe)
- Infotainment
- Maintenance
- Navigation

V2V safety applications will also enable a broader set of safety and mobility applications when combined with compatible roadway infrastructure; therefore V2V serves as the gateway for the broader ITS applications. V2V safety applications that are enabled by V2V alone and could not be replicated, known as vehicle-resident sensor- or camera-based systems are as below.

- Intersection Movement Assist
- Left Turn Assist
- Emergency Electronic Brake Light
- Infrastructure-based devices
- Infrastructure based devices that enable V2I

The figure 4 below describes the overall anticipated system, including V2V and V2I capabilities.
V2I applications include applications for commercial freight operators. V2I applications complement the V2V safety applications by addressing crash scenarios that the V2V cannot address or that could be addressed more efficiently where there are low levels of penetration of DSRC-equipped light vehicles.

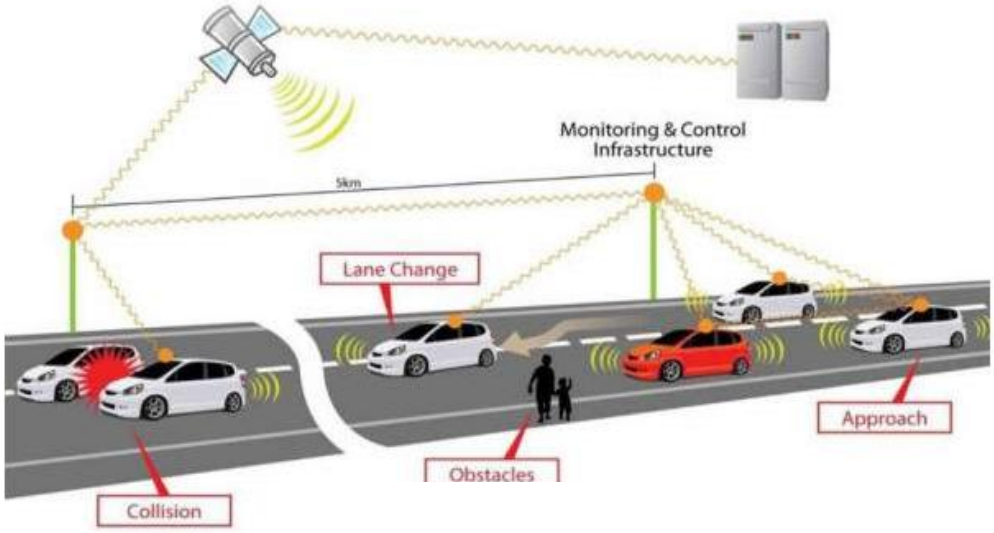


FIGURE 4 OVERALL V2X ARCHITECTURE [1]

3.3.1 V2I potential safety services[2]

The following is a list of V2I potential safety services:

- **Red Light Violation Warning**: The Red Light Violation Warning (RLVW) service aims to increase drivers' alertness at signalised intersections in order to reduce the number and severity of collisions.
- **Curve Speed Warning**: Curve-speed warning (CSW) technology helps drivers to identify potentially dangerous situations if a bend in the road is taken too fast, and warn the driver in advance allowing him time to react properly.
- **Stop Sign Gap Assist**: The Stop Sign Gap Assist (SSGA) safety application is intended to improve safety at non-signalized intersections where only the minor road has posted stop signs.
- **Reduced Speed Zone Warning**: The Reduced Speed Zone Warning (RSZW) application provides connected vehicles which are approaching a reduced speed zone with information on the zone's posted speed limit and/or if the configuration of the roadway is altered (e.g., lane closures, lane shifts).
- **Spot Weather Information Warning**: The Spot Weather Information Warning (SWIW) application will alert drivers to unsafe conditions or road closure at specific points on the downstream roadway as a result of weather-related impacts, which include, but are not limited to high winds, flood conditions, ice, or fog.
- **Stop Sign Violation Warning:** The Stop Sign Violation Warning (SSVW) safety application is intended to improve safety at without signal intersections with posted stop signs by providing warnings to the driver approaching an without signal intersection.
- **Railroad Crossing Violation Warning**: The Railroad Crossing Violation Warning (RCVW) application will alert and/or warn drivers who are approaching an at-grade railroad crossing if they are on a crash-imminent trajectory to collide with a crossing or approaching train.
- **Oversize Vehicle Warning**: The Oversize Vehicle Warning (OVW) application uses external measurements taken by the roadside infrastructure, and transmitted to the vehicle, to support in-vehicle determination of whether an alert/warning is necessary. Specifically, the infrastructure data equipment detects and measures the approaching vehicle's height and width.
- **Red Light Violation Warning**: The Red Light Violation Warning (RLVW) application enables a connected vehicle approaching an instrumented signalized intersection to receive information from the infrastructure regarding the signal timing and the geometry of the intersection.

3.3.2 V2V potential safety services[3]

The following is a list of V2V potential safety services:

- **Control Loss Warning:** The Control Loss Warning (CLW) application enables a vehicle to broadcast a self-generated, control loss event to surrounding vehicles.
- **Motorcycle Approaching Indication:** The Motorcycle Approaching Indication application is intended to warn the driver of a vehicle that a motorcycle is approaching. The motorcycle could be approaching from behind or crossing at an intersection.

- **Pre-crash Actions:** The Pre-crash Actions (PCA) application enables a vehicle to mitigate the injuries in a crash by activating countermeasures in the vehicle when a crash is about to happen.
- **Vehicle Emergency Response:** The Vehicle Emergency Response (VER) application provides public safety vehicles with information from connected vehicles involved in a crash. Emergency responders need information about the vehicles involved in a crash to respond safely and effectively to the vehicle crash.
- **Panic button:** alerts the nearby vehicles in case of a panic within the vehicle.

3.3.3 List of Public & Private Safety applications

The table below shows the V2X services for Public and Private Safety:

TABLE 1 APPLICATION

Public Safety	Private Safety
• Approaching emergency vehicle (warning) • Emergency vehicle signal pre-emption road condition warning • Low bridge warning • Work zone warning • Imminent collision warning • Curve speed assistance [rollover warning] • Infrastructure based – stop light assistant • Intersection collision warning/avoidance • Highway/rail [railroad] collision avoidance • Cooperative collision warning • Green light - optimal speed advisory • Cooperative vehicle system – platooning • Cooperative adaptive cruise control • Vehicle based probe data collection • Infrastructure based probe data collection • Infrastructure based traffic management – • Toll collection • Traffic information • Transit vehicle data transfer (gate) • Transit vehicle signal priority • Emergency vehicle video relay • Mainline screening • Border clearance • On- board safety data transfer • Vehicle safety inspection • Driver's daily log	• Access control • Drive- thru payment • Parking lot payment • Data transfer / info fuelling ➢ diagnostic data ➢ repair- service record ➢ vehicle computer program updates ➢ map and music data updates ➢ video uploads • Data transfer / cvo / truck stop • Enhanced route planning and guidance • Rental car processing • Unique cvo fleet management • Data transfer / transit vehicle (yard) • Transit vehicle refuelling management • Locomotive fuel monitoring • Data transfer / locomotive

3.4 Technology Solutions for V2X

3.4.1 5.850 -5.925 GHz WAVE (DSRC)

Dedicated Short Range Communications (DSRC) is two-way wireless communication envisioned for automotive use, with interoperability between vehicles (V2V) and the traffic signal infrastructure (commonly called V2I) built upon IEEE 802.11p Wireless Access for Vehicular Environments (WAVE) and architecture, security and message protocols standards (IEEE 1609.x in the US and a host of ETSI facilities layer standards). There are ETSI and SAE message set standards, as well as corresponding data elements from infrastructure operators.

While the term "DSRC" is commonly used in North America and Asia, it is referred in Europe as the ITS G5 band to differentiate the 5.9 GHz "V2X" band from 5.8 GHz tolling. This 5.8 GHz tolling is called DSRC in Europe and elsewhere. Moreover, the use of 5.9 GHz is not standardized; in the United States 75 MHz of licensed, free spectrum is allocated across seven half-clocked 10 MHz bands (two of which are safety channels), whereas in Europe 30 MHz is allocated to ITS G5. Other regions of the world do not have such frequency allocations. This brings forward that despite interference and mitigation arguments in Europe, spectrum sharing (with U-NII-4) and security concerns, there is in the United States and Europe, strong arguments but not absolute certainty that 5.9 GHz versions DSRC will be deployed. There is less certainty for 5.9 GHz deployment in other regions of the world [4].

However, DSRC is the only solution available as on date which provides the following features:

- **Fast Network Acquisition**: Active safety applications require immediate establishment of communication.
- **Low Latency**: Active safety applications must execute in the smallest amount of time possible.

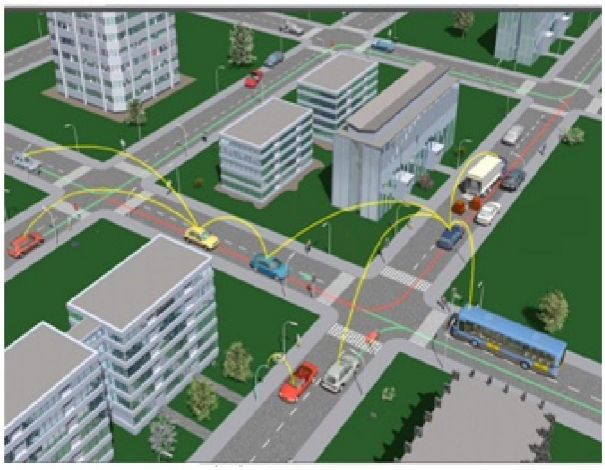


FIGURE 4 DSRC IMPLEMENTED SCENARIO

- **High Reliability when Required**: Active safety applications require high level of link reliability.
- **Priority for Safety Applications**: Safety applications on DSRC are given priority over non-safety applications.

- **Interoperability**: DSRC ensures interoperability, which is the key to successful deployment of active safety applications.
- **Security and Privacy**: DSRC provides safety message authentication and privacy.
  Dedicated Short Range Communications (DSRC) are the communications media of choice for communications-based active safety systems research because:
  - It operates in a licensed frequency band.
  - It provides a secure wireless interface required by active safety applications.
  - It supports high speed, low latency, short-range wireless communications.
  - It works in high vehicle speed mobility conditions.
  - Its performance is immune to extreme weather conditions (e.g. rain, fog, snow, etc.). It is designed to be tolerant to multi-path transmissions typical with roadway environments.
  - It supports both vehicle-to-vehicle and vehicle-to-infrastructure communications.

3.4.1.1 Comparison between DSRC & Others

How DSRC is different from other radio communications may be inferred from the comparative statement in Table 2 below.

TABLE 2 COMPARISON BETWEEN DSRC & OTHERS

	DSRC	**Cellular Phone(up to 3G)**	**Satellite**
Range	100 ~ 1000 meters	Kilometers	Thousands of kilometers
Data Rates	6 to 27 mbps	2-3 mbps	
Latency	200 micro seconds	1.5 ~ 3.5 seconds	10 ~ 60 seconds

3.4.2 Long Term Evaluation (LTE)

A Long Term Evolution (LTE) network is a type of wireless communications network designed to provide broadband Internet and phone service to mobile phones and other types of devices. Voice calls on an LTE network are converted into small chunks of data, which eliminates the need for separate voice circuits. These types of networks are often marketed as "4G" and are capable of offering speeds that rival wired broadband services. They also offer increased capacity, which may help wireless carriers deal with the increasing amounts of data used by smart phones and other devices.

Depending on the spectrum available, live LTE networks can deliver very fast data speeds of up to 100Mbps in the downlink and 50Mbps in the uplink. Designed to be backwards-compatible with GSM and HSPA, LTE incorporates Multiple In Multiple Out (MIMO) technology, the Orthogonal Frequency Division Multiple Access (OFDMA) air interface in the downlink and Single Carrier FDMA in the uplink. This combination provides high levels of spectral efficiency and network performance, coupled with high network capacity and low latency. LTE will support spectrum channel bandwidths from 1.4 MHz to 20 MHz and can operate in both paired spectrum (in FDD mode) and unpaired spectrum (in TDD mode).

Although both LTE and WiMAX use the OFDMA air interface, LTE's compatibility with existing GSM and HSPA networks enables mobile operators to continue to provide a seamless service across LTE and existing deployed networks.

LTE networks have now been launched by mobile operators Europe, Asia and North America.

3.4.2.1 The Benefits of LTE

- Provides a global ecosystem with inherent mobility
- Offers easier access and use with greater security and privacy
- Dramatically improves speed and latency
- Delivers enhanced real-time video and multimedia for a better overall experience
- Enables high-performance mobile computing
- Support real time applications due to its low latency V2V create a platform upon which to build and deploy the products and services of today and those of tomorrow.

3.4.2.2 LTE Device to Device (D2D)

LTE D2D communications is a peer to peer link which does not use the cellular network infrastructure, but enables LTE based devices to communicate directly with one another when they are in close proximity.LTE device to device communication is also being investigated for applications where peer discovery is required for commercial applications in the presence of network support.

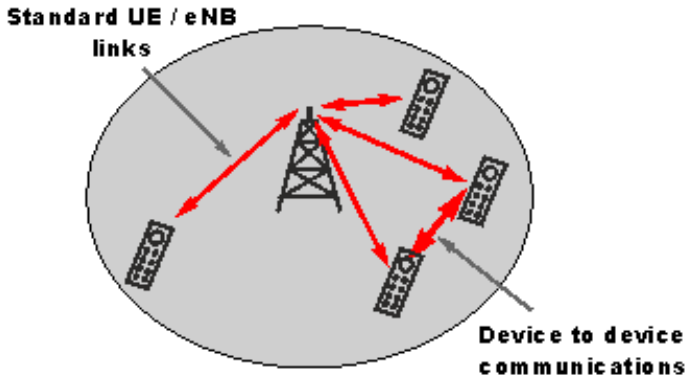


FIGURE 5 LTE DEVICE TO DEVICE, D2D CONCEPT

Integrating D2D into the LTE-Advanced system offers the prospect of a spectrum-efficient, energy-efficient and secure solution for proximity discovery and device-to-device communication, which would benefit from the LTE eco-system of spectrum, mobile devices and network equipment. Some of the potential benefits of LTE D2D include [5]:

A. **Data rates:** Devices may be remote from cellular infrastructure and may therefore not be able to support high data rate transmission that may be required

B. **Reliable communications:** LTE Device to Device can be sued to communicate locally between devices to provide high reliability communications especially if the LTE network has failed for any reason - even as a result of the disaster.

C. **Use of licensed spectrum:** Unlike other device to device systems including Wi-Fi, Bluetooth, etc, LTE would use licensed spectrum and this would enable the frequencies to be used to be less subject to interference, thereby allowing more reliable communications.

D. **Power saving**: Using device to device communication provides energy saving for a variety of reasons. One major area is that if the two0 devices are in close proximity then lower transmission power levels are required.

E. **Spectrum reuse**. D2D could enable even tighter reuse of spectrum than can be achieved by LTE small cells, by confining radio transmissions to the point-to-point connection between two devices.

F. **Security**. D2D can take advantage of the key generation and distribution mechanisms already available in LTE, to achieve high levels of security.

DSRC is based on IEEE 802.11p and is now 15 years old and mainly deployed in US and Europe. LTE will have the features of LTE direct in 3GPP Release 12. LTE Direct is improved in 3GPP Release 13 and further improvements will be in Release 14. As a DSRC bearer protocol, LTE Direct can be used perfectly in the 5.9 GHz allocation. Standards in release 13 are expected to be frozen in 2016 and release 14 in 2017. The actual implementation of release 14 may happen in India around 2020.

3.4.3 Other technologies

For V2V Communication, there are two more Technologies that have been at an advanced stage of development and Trials: 1) Automotive Short-range radar (SRR) working on 24GHz & 79GHz; and 2) IEEE802.11ad based mm wave WLAN at 60GHz…

Surface transportation safety can be enhanced by the use of wireless technologies, mainly automotive radar and vehicle-vehicle (V2V) communication. Automotive radar provides a high-resolution low-latency approach for a continuous automatic detection and ranging of both, communication-enabled and non-communication-enabled transportation users. V2V systems rely on the collaborative communication between vehicles to achieve a real-time cooperative detection and ranging. They can operate beyond the line-of-sight constraints of radar solutions. Combining both these wireless technologies would provide hybrid detection and ranging application that would benefit from mutual sharing of information between radar and communication using the same frequency band and hardware resources. Furthermore, using mm Wave band will provide a high data rate for communication and better accuracy & resolution for radar operation. This will enable automotive safety applications to simultaneously achieve ultra-low latency and high range of operation, with advantages of reduced cost, size, better performance and efficient spectrum usage for the vehicles of tomorrow.

Recently, developers have leveraged the use of a mm Wave wireless local area network (WLAN) standard to develop a combined vehicular communication-radar waveform. In particular, this will exploit the use of the special structure (repeated Golay complementary sequences) of the single carrier preamble in IEEE 802.11ad to develop a joint framework of long-range automotive radar (LRR) and vehicle-to-vehicle communication (V2V) at 60 GHz. This framework leverages the signal processing algorithms used in the typical WLAN receiver, e.g. carrier frequency offset estimation and channel estimation for radar parameter estimation. The initial results show that the IEEE 802.11ad waveform works well for radar.

Another V2V technology - Automotive short-range radar (SRR) uses the electromagnetic field distribution around a vehicle including reflection from other objects to detect obstacles. If the vehicle is moving the radars can warn the driver to possible impacts and even automatically trigger safety devices such as seat belts or air bags. One of the biggest challenges on the design of SRR is the high frequency of operation, which makes it difficult the use numerical simulation due to the small wavelength, leading to electrical large models. SRR works on 24 GHz and 79 GHz bands. The 79 GHz band is considered to be the long-term operating frequency for SRR.

3.4.4 Observations

DSRC works on 5.8-5.9 GHz and is the only available solutions at present. However it should work only on dedicated spectrum to avoid any interference as well as the security issues. 3GPP release 12 which talks about LTE direct and further improvements have been proposed in release 13 and 14 make take 7-10 years in implementation in India in V2X. However 5G will be the ultimate solution

for V2X communication. The standards for 5G will be frozen in 2020 and may take further 5 years for implementation.

In future it is proposed that LTE may work in two bands simultaneously, the normal operating band and as well as 5.9 GHz band to support DSRC.

3.4.5 Snapshot of the work going in ITU

ITU-R document has compiled comparative study of standards developed by ETSI, IEEE,ARIB and TTA. It has recommended use of radio interface as mentioned in above Table foe V2V and V2I communication. Comparison of Technical characteristics of each standard is shown in Table 4.

TABLE 3 TECHNICAL CHARACTERISTICS

Parameter	ETSI	IEEE	ARIB	TTA
Operating frequency range	5855– 5925 MHz	5 850–5 925 MHz	755.5–764.5 MHz (Single channel)	5855–5925 MHz (Pilot system)
RF channel bandwidth	10 MHz	10 MHz or 20 MHz	Less than 9 MHz	Less than 10 MHz
RF Transmit Power/EIRP	Max 33dBm EIRP		-	23 dBm
RF transmit power density			10dBm/MHz	
Modulation scheme	BPSK OFDM, QPSK OFDM, 16QAM OFDM, 64QAM OFDM	64-QAM-OFDM 16-QAM-OFDM QPSK-OFDM BPSK-OFDM 52 subcarriers	BPSK OFDM, QPSK OFDM, 16QAM OFDM	BPSK OFDM, QPSK OFDM, 16QAM OFDM, Option: 64QAM
Forward error correction	Convolutionalcoding, rate = 1/2, 3/4, 2/3	Convolutionalcoding, rate = 1/2, ¾	Convolutionalcoding, rate = 1/2, 3/4	Convolutional coding, rate = 1/2, 3/4
Data transmission rate	3 Mbit/s,4.5 Mbit/s, 6 Mbit/s, 9 Mbit/s, 12 Mbit/s, 18 Mbit/s, 24Mbit/s, 27Mbit/s	3, 4.5, 6, 9, 12, 18, 24 and 27 Mbit/s for 10 MHz channel spacing 6, 9, 12, 18, 24, 36, 48 and 54 Mbit/s for 20 MHz channel spacing	3 Mbit/s,4.5 Mbit/s, 6 Mbit/s, 9 Mbit/s, 12 Mbit/s, 18 Mbit/s	3, 4.5, 6, 9, 12, 18Mbit/s, Option: 24, 27 Mbit/s
Media access control	CSMA/CA	CSMA/CA	CSMA/CA	CSMA/CA, Option: Time Slot based CSMA/CA
Duplex method	TDD	TDD	TDD	TDD

3.5 Types of V2V devices

3.5.1 OEM Devices

An OEM device is an electronic device built or integrated into a vehicle during vehicle production. An integrated V2V system is connected to proprietary data busses and can provide highly accurate information using in-vehicle information to generate the Basic Safety Message (BSM). The integrated system both broadcasts and receives BSMs. In addition, it can process the content of received messages to provide advisories and/or warnings to the driver of the vehicle in which it is installed. Because the device is fully integrated into the vehicle at the time of manufacture, vehicles with Integrated safety systems could potentially provide haptic warnings to alert the driver (such as tightening the seat belt or vibrating the driver's seat) in addition to audio and visual warnings provided by the aftermarket safety devices. Potential applications of such devices in a scooter are shown in Figure 6.

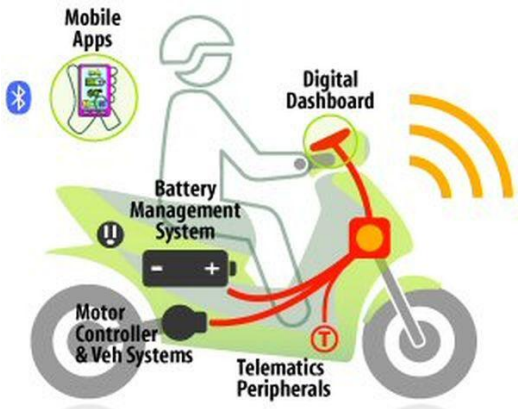


FIGURE 6 OEM DEVICE IN SCOOTER

3.5.2 Aftermarket Devices

Automotive aftermarket devices can be defined as any product with one or more functions in the areas of comfort, convenience, performance, or safety, which are added to a motor vehicle after its original assembly. An aftermarket V2V communication device provides advisories and warnings to the driver of a vehicle similar to those provided by an OEM-installed V2V device. These devices, however, may not be as fully integrated into the vehicle as an OEM device, and the level of connection to the vehicle can vary based on the type of aftermarket device itself. Types of aftermarket devices are shown in Table 3 below:

TABLE 4 AFTERMARKET DEVICES

S.N.	Device Type	Definition	Method of Installation	Functionality
1	Vehicle Awareness Device	Device is able to be connected to the vehicle for power source. Device provides Basic Safety Message for surrounding vehicles.	Device would need to be installed by a certified installer on vehicles not equipped with V2V technology to ensure correct antenna placement and security.	• Transmits BSM

S.N.	Device Type	Definition	Method of Installation	Functionality
2	Aftermarket Safety Devices (i.e., Self-contained)	Device is connected to the vehicle for power source, Device transmits BSM and receives BSMs to support safety applications for the driver of the vehicle in which it is installed.	This device only receives power from the vehicle; however, a certified installer would need to ensure correct antenna placement and security.	• V2V Safety applications • Receives and Transmits BSM • Driver-Vehicle Interface
3	Retrofit Safety Devices	Device is connected to the vehicle's data bus that provides BSM and safety applications for the driver of the vehicle in which it is installed.	This device needs to be connected to the vehicle's data bus, therefore would require an installer that can access this for the particular make of vehicle. Also, a certified installer would need to ensure correct antenna placement and security.	• V2V Safety applications • Receives and Transmits BSM • Driver Vehicle Interface • Integration into the vehicle data bus

3.6 Indian Initiative

Government of India has embarked on a journey for a unified Electronic Toll Collection (ETC) system across the country's highway network, which would enable toll to be collected electronically from vehicles at toll plazas while the vehicle is in motion. A key component for implementation of Nationwide Radio Frequency Identification (RFID)-based ETC is interoperability, which requires standardization and integration. Typical existing product(s) for 'RFID- based-ETC' operates in the 865 MHz – 867 MHz band [6].

3.7 Recommendations

Keeping in view the fact that Intelligent Transport Systems will need to be implemented not only cities but across adjacent cities and highway and wireless will be medium of communication, following are the recommendations:

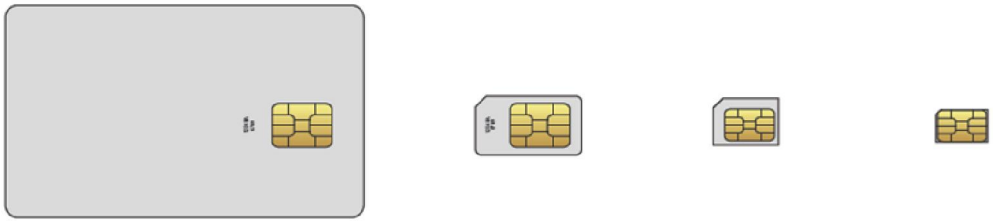
1. To ensure seamless movement and interoperability and smooth development of systems:
    I. Set of technical specifications should be finalised
    II. Technical regulations for enforcement of specifications and other aspects should be finalised
2. While the currently available DSRC standard mostly uses 5.850-5.925 GHz band which is used for satellite communication in India, efforts may be made to identify band of say up to 30MHz (as done in Europe) for ITS. Additional band may also be identified.
3. As the TEC work group have industry wide representation, TEC should take up the work of drawing up specification and technical regulations for implementation of specifications.

4 eUICC & Remote Subscription Management

4.1 Requirements for the eUICC

The GSM Subscriber Identity Module (SIM) has played a very significant role in the proliferation of the GSM services across the globe. Whilst the removable SIM card was perfect for the consumer market and the handsets, it is facing new challenges in the M2M ecosystem. GSMA has published specifications for a new embedded SIM, called the eUICC, and the remote over-the-air (OTA) provisioning of M2M devices which address some of these challenges.

The evolution of GSM SIM cards is shown in Figure 7 below:



Variant	1FF	2FF ("Mini SIM")	3FF ("Micro SIM")	4FF ("Nano SIM")
Year of launch	1991	1996	2003	2012
Dimensions (mm)	85.6 x 53.98	25.0 x 15.0	15.0 x 12.0	12.3 x 8.8

FIGURE 7 EVOLUTION OF THE GSM SIM

Source: GSMA Intelligence based on Justin Ormont's work

The M2M Devices have a requirement for new SIM cards which can be embedded into the Printed Circuit Board (PCB) (see Figure 8: eUICC and the ISO SIM) ubiquitously found in electronic devices. It is likely that the M2M devices will be used in an environment where physical access to the SIM may not be possible, and the removable SIM may not be the most optimum form factor. This brings in a need for 'over the air' provisioning of the SIM with the same level of security as achieved today with traditional removable SIM.

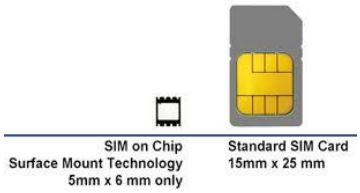


FIGURE 8 EUICC AND THE ISO SIM

The Evolution of the SIM for the M2M devices has led to the development of the new SIM form factor called the MFF1/2 SIM, which is shown here as a SIM on a chip, suitable for Surface Mounting on a PCB.

The MFF1/2 SIM cards are assembled as part the M2M device PCB at the factory stage. The Subscription information is added in the after-market operation. As a result, a new requirement imposed on these SIM cards is that they must be over the air manageable for mobile subscriptions. Without this critical enabler, consumers and OEMs will not be able to select the mobile operator when the device is sold in the market place.

Further, the M2M SIM cards will often be used within devices that are meant for use in industrial and automotive use cases. As a result, these SIM cards must be able to tolerate a harsher ambient environment and have a longer life, commensurate with the devices that they are embedded in.

Another significant change arriving in the M2M domain is the ownership of the M2M SIM. All the SIM cards issued till date belong to MNOs. This is set to change in the IoT/M2M domain. The embedded SIM is more likely to be supplied by an OEM or the M2M Service Provider. A single eUICC can have multiple profiles, each of which can contain connectivity from an MNO. As a result, one eUICC, issued by an M2M Service Provider, can have multiple MNO subscriptions.

An illustrative comparison of SIM card capabilities is presented in Table 5.

TABLE 5 ATTRIBUTES OF THE DIFFERENT SIM FORM FACTORS

SIM Type	Consumer	Industrial	Automotive
Temperature	-25 to +85°C	-40 to +105°C	-40 to +125°C
Data Retention	5 Years	12 Years	15 Years
Removable/Embedded	Removable	Removable/Embedded	Embedded
Owner	Mobile Operator (MNO)	MNO / OEM	OEM

Whilst the introduction of the eSIM brings benefits across the entire IoT / M2M ecosystem, but it also requires significant changes in Standards, Policies and Roles at several points in the value chain. For example, the current regulations in India mandate that the SIM ownership must remain with its custodians – i.e. either with the individual, or with corporates in case of bulk/ corporate connections. Globally in most M2M solution use cases today, the M2M Service Provider (M2M SP) ties up with an MNO, fits the M2M device with an activated removable SIM card issued in the name of the M2M SP and sells the device through its retail chain. However, it is susceptible to tampering and misuse.

Connected M2M objects (Cars, Health Devices, Navigation systems, etc) are sold in the open market, and are subject to resale and transfer in the after-market operation. However, the current rules preclude the transfer of SIMs, which needs be addressed so as to allow the new custodian of the device to take ownership of the M2M device.

India is a hyper competitive market, uniquely broken into 22 Telecom Circles. The vast geography, massive growth in mobile users, limited availability of spectrum and the competition have ensured that no single MNO can service the entire country with all the types of possible accesses (2G/3G/4G). In the recent times, the regulator has been seized with the massive problem of call drops. Mission critical M2M use cases require reliable, continuous and highly available connectivity. The embedded SIM with its capability to host multiple subscriptions can provide a solution to this problem.

A study commissioned by GSMA presented a view that the automotive industry could increase its share of M2M connected cards in 2020 from 158Mn to 252 Mn on account of the eUICC and its ability to hold multiple subscriptions. A graphical representation of growth in use of eUICC based

SIMs till 2020 is given in Figure 9. It also indicates the split in single subscription, dual subscriptions and three subscriptions.

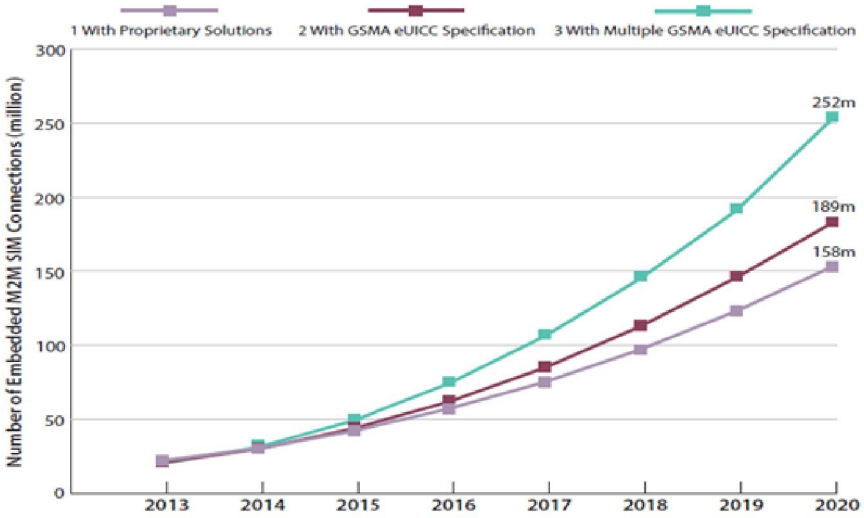


FIGURE 9 GROWTH OF CONNECTED CARS WITH THE GSMA EUICC

Source: Researched and Published by Beecham Research Limited

It is clear that eSIM and remote subscription management are set to play a critical role in proliferation of the IoT / M2M devices and use cases. The priority is the creation of a sustainable M2M regulatory & policy environment that allows the IoT ecosystem to unlock the consumer and business benefits from the new technology.

The GSMA eUICC will require two new Network Nodes to be added to the Mobile Network OR M2M SP OR OEM infrastructure. These are the SM-SR (Subscription Management - Secure Router) and the SM-DP (Subscription Management - Data Preparer).

SM-SR (Subscription Management - Secure Router)

The secure router is the GSMA defined entity (SM-SR), which is responsible for UICC platform management and communication. The SM-SR manages and downloads network access credentials and other confidential MNO subscription data into the UICC in a highly secure way upon request of the customer. The secure router can load, enable, update and delete subscriptions on a UICC over-the-air and in some special cases over the Internet.

The management of the subscription data is handled completely remotely over-the-air, independent of the device and is protected with end-to-end security between the source of the subscription data (i.e. SM-DP) and the unique UICC.

SM-DP (Subscription Management - Data Preparer)

The data preparer is the GSMA defined entity (SM-DP) that is responsible for data preparation of UICC profiles to be downloaded on UICCs already distributed in the field. It generates and handles the mobile operators' mobile network credentials and generates the UICC card profile (files).

The DP stores pre-generated, personalized UICC profiles, which are then, on request, packaged and finalized in real time. The data preparer is batch-provisioned with UICC profile scripts and corresponding personalization data like:

- Mobile network authentication credentials (subscription data)
- Unique UICC and profile identifier
- PIN/PUK/ADM codes etc.
- Operator specific UICC communication encryption keys, OTA, TLS, etc.
- Application and service specific personalization parameters

The profile package is sent to the SM-SR for download. The SM-DP tracks all imported and known subscriptions and manages the anti-cloning database, which ensures that the same personalized profile is not duplicated (downloaded) to several UICCs

4.2 Standards and Inter-operability Requirements: International Scenario

A brief description of the status on this matter is given below:

GSMA

The GSMA has issued Embedded SIM Specifications which provide a single, de-facto standard mechanism for the remote provisioning and management of machine to machine (M2M) connections, allowing the "over the air" provisioning of an initial operator subscription, and the subsequent change of subscription from one operator to another.

GSMA has published a set of documents to assist the standardisation of the eUICC and the Remote Subscription Management, some of which are listed below:

- Embedded UICC Consumer Protection Profile
- Remote Provisioning Architecture for Embedded UICC Technical Specification Version 3.0 June 2015 Version
- GSMA Embedded SIM Remote Provisioning Architecture Version 1.1
- Remote Provisioning Architecture for Embedded UICC Technical Specification Version 2.0
- 2014Business Processes for Remote Provisioning in M2M

The GSMA description of the embedded SIM is reproduced in Figure 10 below

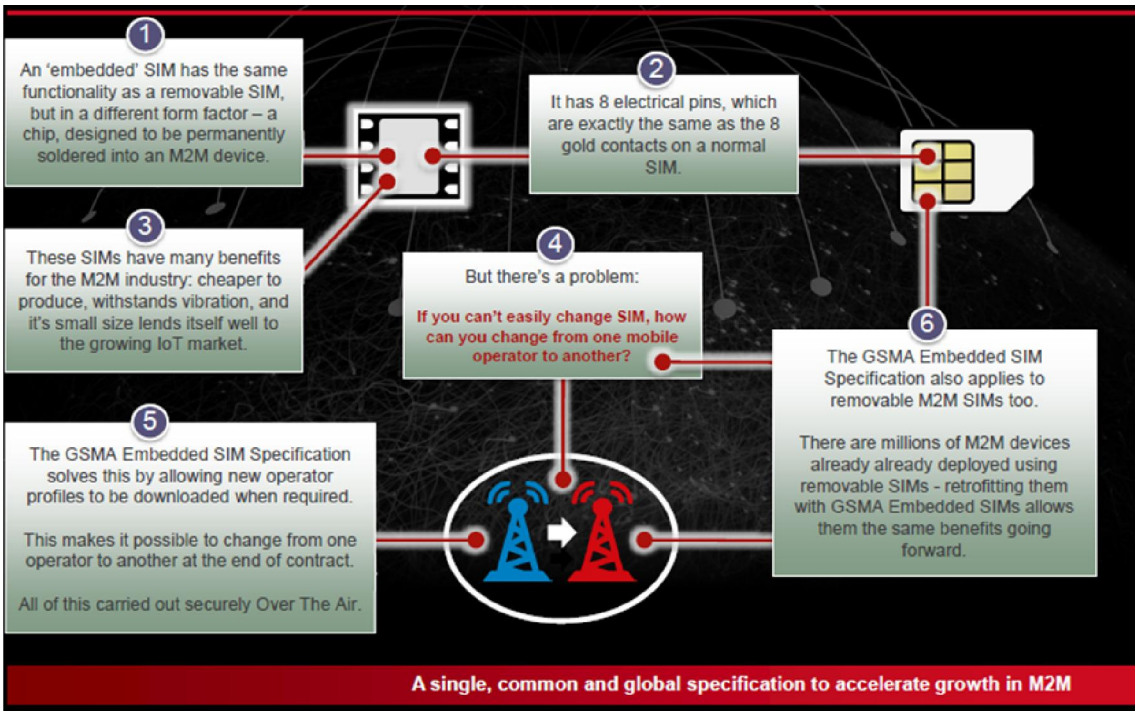


FIGURE 10 THE EMBEDDED SIM

Source: GSMA, Connected Living:A single, common and global specification to accelerate growth in M2M

For the eUICC to be successful, interoperability is a key requirement, both between GSM MNOs and the GSM SIM suppliers. The Figure 11below shows the expectation from this standpoint.

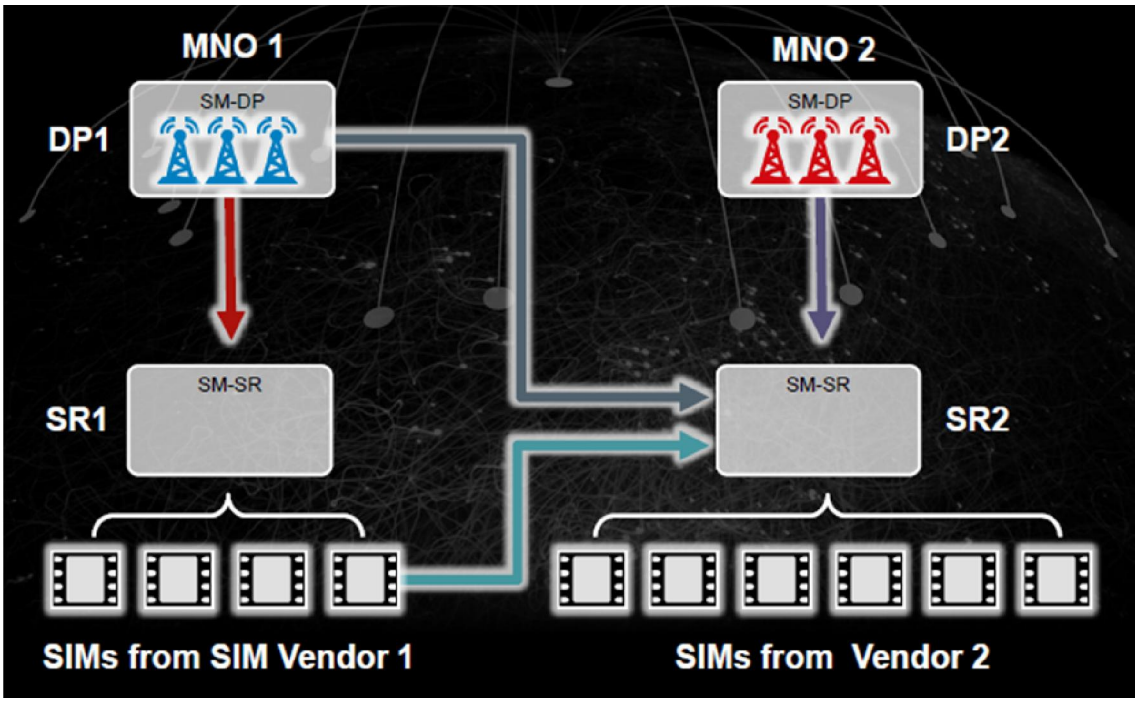


FIGURE 11 SUBSCRIPTION MANAGEMENT WITH THE EMBEDDED SIM

Source: GSMA, Connected Living: A single, common and global specification to accelerate growth in M2M

The GSMA has released an Embedded SIM Test Specification, the purpose is to ensure products made by vendors, including eUICC, SM-DP and SM-SR entities are functionally compliant to the GSMA Embedded SIM Technical Specification.

The GSMA has extended its successful Security Accreditation Scheme (SAS) to cover remote provisioning subscription management service to ensure that the robust security and product integrity requirements are maintained.

The adherence to security standards is a critical requirement, towards which, a Certificate Issuance process has been specified. The Certificate Issuer (CI) process ensures that the various system entities (SM-DP, SM-SR, EUM, eUICC) can all be trusted by each other. Whilst the GSMA will be the Sole Certificate Issuer initially, other Certificate Issuers will have to be added in a hierarchy, as the market matures.

ETSI

The European Telecommunications Standards Institute's Technical Committee on Smart Card Platform has released a Requirements Specification Titled Smart Cards; Embedded UICC with a Release 12 of the document number ETSI TS 103 383 V12.0.0 (2013-02).

The ETSI Technical Specification has the following to say in its introduction

> "Work on Machine-to-Machine (M2M) applications has given rise to the possibility of having a UICC that is embedded in a communication device in such a way that the UICC is not easily accessible or replaceable. The ability to change network subscriptions on such devices

becomes problematic, thus necessitating new methods for securely and remotely provisioning access credentials on these Embedded UICCs (eUICC) and managing subscription changes from one MNO to another. In its current state, the present document is to be considered as a "work in progress". It contains a restricted set of requirements related to the provisioning of profiles in an eUICC as well as general requirements on the architecture of the eUICC. As a consequence, some of the elements required to specify a complete technical solution are missing, among which are requirements for:

• management of profiles;

• management of credentials;

• the policy control function;

which will be defined in further versions of the present document."

The specifications for the implementation of the eUICC and its Remote Subscription Management basically cover the following aspects

- Specification of two new key network elements – the SM-DP and the SM-SR
- The remote over the air provisioning of a one (or more) operator profiles into a SIM
- The remote over the air enablement / disablement of an operator profile within the SIM, thus enabling a change of active operator
- Over the air deletion of an operator profile within a SIM
- facilitate the secure over the air management of mobile operator credentials within a SIM

3GPP

The M2M applications based on UICC platform are defined in 3GPP technical Specifications (Release 9 or above) for automobile industry.

The list of applicable standards of ETSI & 3GPPis presented in Table 6 below

TABLE 6 STANDARDS RELATED TO THE EUICC AND ITS SUBSCRIPTION MANAGEMENT

S. No.	Standard Name / Number	Version
1	ETSI TS 101 220 Smart Card ETSI Numbering system for telecommunication application provider	8.4.0
2	ETSI TS 102 221 Smart cards; UICC-Terminal interface; Physical and logical characteristics	8.2.0
3	ETSI TS 102 222Universal Integrated Circuit Cards (UICC); Administrative commands for telecommunications applications	7.0.0
5	ETSI TS 101 116 V7.0.1 (1999-07): Digital cellular telecommunications system (Phase 2+); Specification of the 1.8 Volt Subscriber Identity Module Mobile Equipment (SIM - ME) interface (GSM 11.18 version 7.0.1 Release 1998)	7.0.1
6	3GPP TS 31.101 V5.2.1 (2004-12): 3rd Generation Partnership Project; Technical Specification Group Terminals; UICC-terminal interface; Physical and logical characteristics (Release 5)	5.2.1

7	3GPP TS 31.102 V5.15.0 (2012-09): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Characteristics of the Universal Subscriber Identity Module (USIM) application	5.15.0
8	ETSI TS 102 221 Smart Cards; UICC-Terminal interface; Physical and logical characteristics	V8.5.0
9	ETSI TS 151 011Smart Cards; Smart Card Platform Requirements Stage 1	V8.4.0
10	ETSI TS 102 225 Smart Cards; Secured packet structure for UICC based applications TECHNICAL SPECIFICATION	V8.5.0
11	ETSI TS 102 226 Smart Cards; Remote APDU structure for UICC based applications	V8.3.0

It is noted that TEC has issued specifications for eUICC. These will need to be extended to cover the requirements of automotive sector also. In addition, Specifications for Certificate Issuers will need to be drafted in conjunction with the GSMA, as GSMA readies to delegate these per region, or country or even market sector.

A set of recommendations for a future Interface Requirement for the eUICC are stated in Annexure A.

4.3 Considerations for deployment of the eUICC

The deployment of the eUICC shall impact players across the value chain in several prominent industries, including the automotive. The M2M Ecosystem Value Chain is shown in Figure 12.

FIGURE 12 THE M2M ECOSYSTEM VALUE CHAIN

The following critical aspects must be kept in mind in the development of Standards, Policies and Guidelines for the eUICC and Subscription Management:

- Interface Requirements for the eUICC
  - Reserved space for Government Apps within the eUICC
- Hosting of the new Network Nodes – SM-DP and SM-SR
- Appointment of a local Certificate Issuer(s) and local Certification Agency in conjunction and agreement with the GSMA as per a hierarchy of delegation agreed with GSMA
- Defining a hierarchy of Certificate Issuer(s) and Certification Agency such as to recognise the distinct capabilities and management required for
  - the Secure Element
  - the eUICC

Security& Privacy

- Location of Application Servers
- Location of SM-DP; SM-SR
- Transfer of Devices with Embedded SIM cards using eKYC
- Preventing the misuse of identity by masking the MSISDN

Quality of Service

- M2M SIM Roaming guidelines
- Leverage the eUICC capability to host multiple MNO subscriptions
- Processes for use of multiple Subscriptions within a single device to improve access

Processes for Subscription Management

- The role of the M2M Service Provider as envisaged under the National M2M Roadmap
- Numbering and Identification of the eUICC pools per M2M SP

4.3.1 Synergy with international standards and M2M standard endorsed by DoT

It is important that specification in India are consistent with other SDOs and the Standards endorsed by DoT.

China Telecom and Huawei submitted a requirement to OneM2M, WG1, on the matter of "M2M Service Provisioning for Equipment with Built-in M2M Device" which is relevant to this recommendation.

The relevant extract from contributions is as below:

> *''This contribution mainly focuses on M2M service provisioning in the above case. M2M service consists of the service provided by M2M service platform and network service provided by the mobile network. Therefore, full M2M service provisioning consists of M2M service provisioning and network service provisioning. The former is to allow M2M device to talk with M2M service platform. The latter is to make M2M device access mobile network.*
> *M2M service platform is operated by M2M Service Providers (M2M SP). With M2M SP's help, Equipment Providers don't need to manage mobile-network specific identifiers, such as IMSI, MSISDN or MDN. They just use Equipment ID / Equipment Name and Device ID / Device Name to identify equipment and device.*
> *M2M Service Platform can hide the complexity of the underlying mobile network. It can provide standard interface for equipment providers' applications to activate or deactivate M2M service of specified equipment / M2M device. Not only will it active or de-active M2M Service provided by M2M Service Platform, but also it will talk with underlying network to activate or deactivate network service provided by mobile network."*

4.3.2 Ownership Transfer through e-KYC

Addressing the key challenges referred in document TR: M2M enablement in ITS (TEC-TR-S&D-M2M-003-01) extract:
KYC norms for the SIM being used in ITS Devices (GPS/ GPRS etc.) need to be different than the KYC norms for SIM being used for mobile phone. Currently, there is no mechanism to ensure vehicle ownership transfer is in sync the device SIM connection, which needs to be addressed.

It is evident that accidents, theft and traffic can be much better managed if the automobiles on the roads were tracked for their location, speed and driving behaviours. This can be achieved if vehicles are factory fitted with tamper proof telematics devices. A significant barrier to this is the need for an embedded SIM ecosystem.

It is proposed that an M2M Service Provider is permitted to provide embedded SIM connections, so that the factory-fit lifecycle of the eUICC can be managed. It is further proposed that the buyer of the automobile is provided a user friendly mobile and web application such that an Aadhaar based e-KYC or an IT Act supported Digital Signature can be performed, and the connection registered in the name of the buyer of the vehicle. The M2M Service Provider must provide regular updates to the authority it is registered with, as required by the guidelines issued by the competent authority.

In addition to the above, Registration of an automobile be done by respective registrar /authority through eKYC. This will improve the authenticity of customer; quick activation/ profile download of SIM. Such option will empower the authority with more knowledge about registrant and will improve traceability of registrant if need arises addressing country level security concerns. Typical eKYC process for automobile is given in Figure 13.

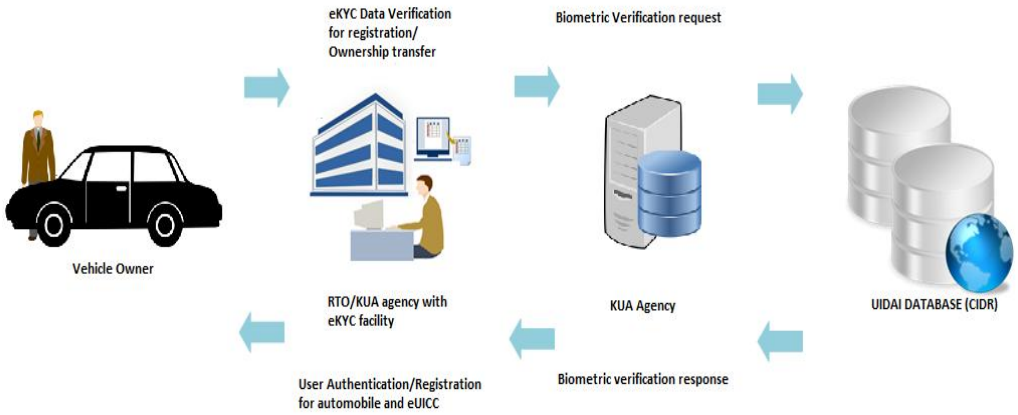


FIGURE 13 EKYC PROCESS FOR EUICC PROVISIONING

The eKYC process enables quick and paperless transfer of the ownership of the subscription from the Service provider to the user and then from one user to another

4.3.3 Security & Privacy

While building M2M networks, connectivity and physical location of various elements is equally important. However one should also bear in mind the privacy of the user. It is recommended that the best practices of anonymization of customer identity be followed. so that the original identity of the individual is not revealed, without user consent or unless it involves National security

Further,keeping in view the variety of M2M services, a policy decision regarding hosting of data in India needs to be taken

4.3.4 Quality of experience monitoring and troubleshooting services

Since mobile operators have to transparently manage multi-access networks (2G, 3G, LTE, Wi-Fi) and are moving to all-IP architectures, ensuring a high quality of service becomes a new and real challenge to acquire and retain customers who have high expectations and are more and more used to anytime, anywhere, seamless and transparent access to mobile services. The eUICC can turn into a tool which, no matter what kind of network issue prevents connection (network congestion, network failure, service not subscribed, etc), provides tailored and real-time solutions to the issues that affect the customer experience. In the hands of the M2M Service Provider, the multi-subscription capability of the eUICC can significantly improve the quality of M2M services.

4.3.5 Emergency Call (E-Call)

This recommendation is meant for Automotive Research Association of India.

An Emergency Call feature, or E-Call as it is popularly known, is a feature mandated by several European countries. When a motorist encounters an emergency situation he\she should be able to connect to the emergency services via the device either automatically or manually for roadside assistance.

ERA Glonass is a Russian standard similar to the European eCall to combine mobile communications and satellite positioning to provide rapid assistance to motorists in the event of a collision. To fulfil the ERA Glonass requirements some extensions of the GSMA's Remote Provisioning needs to be done.

- **Specific card profile for emergency case**

There shall be a specific profile, which should be used in case of an emergency. This profile needs to be configurable and be automatically activated in case of an emergency.

- **Quick activation of the emergency profile**

In case of an emergency the device shall be able to activate the specific profile to setup an emergency call in the ERA Glonass system. This switch shall be done as fast as possible to save time and providing a fast rescue.

- **Assurance of an operation without interruptions**

During the emergency case there shall be no interruptions to ensure that the emergency call will be done properly. This shall be handled by the device itself as the device is the entity with the most control over the situation.

4.3.6 M2M Roaming

Present licensing regime allows licensees to enter into roaming agreements with other licensees as per their commercial arrangements for national roaming. For international roaming, licensees can enter into agreements with foreign telecom Service Providers to provide roaming facility to its subscribers & vice versa. Roaming subscribers can only access services to which they have subscribed in their home networks. The guidelines are applicable to voice as well data services.

There are concerns on non-availability of M2M services in North Eastern States and J&K in case of imported devices pre-fitted with foreign SIM cards. This is due to restrictions placed on international SIMs roaming to these areas. As government is considering only Indian SIM to be used in M2M devices, this may not remain an issue.

4.3.7 Embedded UICC Application frame work

It is recommended that USIM may reserve up to 32K of Non Volatile Memory (NVM) and 1K of RAM space to be used for uploading Government specific applications like; Disaster management system, social welfare system for health and safety etc.

4.3.8 Location Enablement, personalized and differentiated services

Mobile internet is about providing tailored and location-aware applications to satisfy end users' expectations. The LTE UICC allows the creation of new GPS-based location-based services and provides the path to securely deploy third-party applications and services with no need for additional provisioning of access parameters and shared security keys.

The eUICC capabilities include:

- Obtaining the location data from a GPS-enabled handset in order to enhance the information of menu-based browsers, to define “geo fences” for location-based advertising, etc.
- Establishing the secure connection between the eUICC and a third-party remote server for the distribution of broadcasted content with a pay-per-use business model.

4.3.9 Usage of the Cloud for eUICC enabled M2M Applications

To harness the full potential of M2M, Cloud usage plays a major role. Favourable cloud use guidelines are required to be worked out at the earliest. In this regards, future M2M guidelines may consider the following:

I. Cloud based M2M services should be inter-operable and comply with open-standards i.e the API used for information exchange between the device and the platform to be standardized and the all stakeholders should comply with them ensuring interoperability

II. The document OneM2M specifying the use of OMA DM and OMA LWM2M should be followed by all stakeholders

III. Lawful interception shall be supported as per prevailing norms.

IV. As the number of connected devices would increase gradually IPv6 support should be built right from beginning as this would ensure identity and better security

4.4 Recommendations

Keeping in view the eUICC requirements for automotive sector and regulatory issues which need to be addressed as brought out in the report; following are the recommendations that can assist the framing of the Regulations and Policies in the area of eUICC and Remote Subscription Management:

1. Interface requirements of TEC for eUICC may be amended to incorporate the requirement of automotive sector including remote subscription management, multiple subscription and eUICC enabled location identifications.

2. Regulatory policies/ guidelines may be evolved on the following:

    I. The issuance of Embedded SIMs by OEMs / M2M Service Providers, and the Identification of M2M SP / OEM by IMSI ranges
    II. Transfer of "Devices with Embedded SIMs" from one user to another using AADHAAR eKYC
    III. In conjunction with GSMA, development of Policy Guidelines for setting up Indian Certificate Issuers and local Certification Agencies for the new Network elements for the eUICC
    IV. M2M Roaming
    V. M2M / IoT privacy and security including the subjects of location of Application Servers hosting user data, use of MSISDN as an identity, IPV6 mandate such as to ensure a unique identity per connected SIM

3. Assign a priority for release of E-Call requirement by appropriate agencies such as the ARAI.

Annexure A

Recommendations for eUICC and Remote Subscription Management Requirements

eUICC

1. eUICC Architecture

The eUICC architecture is based on telecommunication standards and Global Platform standards which aid to establish role separation and data isolation so that each entity has a dedicated Security Domain with different privileges and configuration.

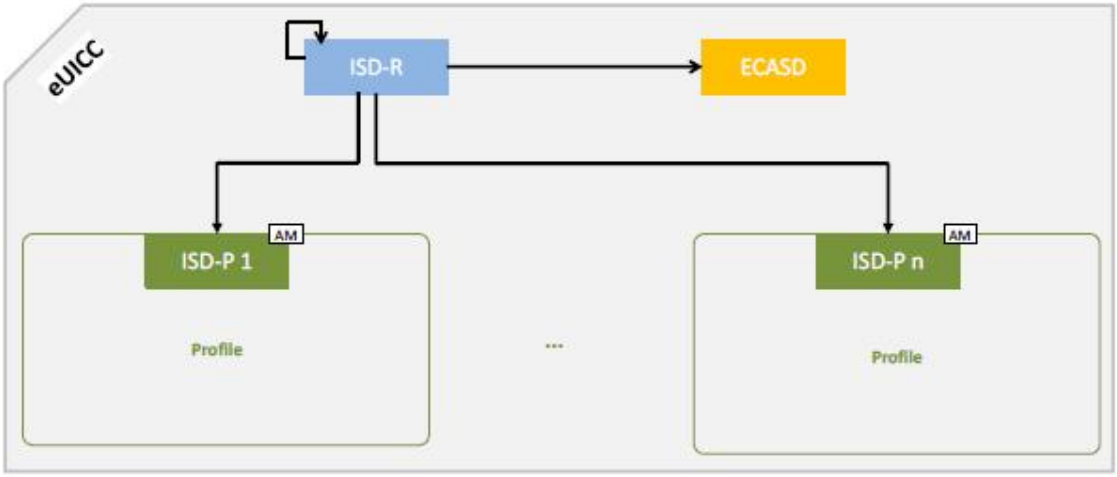


FIGURE 13 EUICC ARCHITECTURE

COMPONENTS OF EUICC:

a. The operating system (OS) contains the basic platform features, e.g. support of the features defined in the Global Platform Card Specification [GPCS].
b. The ECASD (eUICC Certificate Authority Security Domain) is created within a eUICC at time of manufacture; it cannot be deleted or disabled after delivery. It contains a non-modifiable eUICC private key, the associated Certificate, the CI's root public keys and the EUM keyset for key/certificate renewal.
c. ISD-R and ISD-P are security domains with special features.
d. The ISD-R (ISD-Root) is the on-card representative of the SM-SR that executes the Platform Management commands. This function can belong to MSP or M2M Service Provider.
e. The ISD-P (ISD-Profile) is the on-card representative of the MSP, or SM-DP if delegated by the MSP. The delegation of the MSP can be an M2M Service Provider.
f. The MSP-SD is the on-card representative of the MSP or the M2M Service Provider.
g. The SM-DP performs the Profile Management functions on the ISD-P during the load and install phase.
h. Contained in the ISD-P are the well-known card structure with applications, SDs for other entities, the file system (MF tree, ADFs, etc.) (As per ETSI TS 102 221 and 3GPP TS 31 102) and the Policy Rules.

SECURITY DOMAINS

The eUICC architecture comprises the following Security Domains for the purpose of Platform and Profile Management:

- Secure storage for cryptographic keys
- Access for off card entities using (GP) secure channel protocols
- A mechanism for loading applications
- Security services for applications.

PROFILE STRUCTURE

The Profile structure shall include:

- The MSP-SD, where the MSP can be substituted by a M2M Service Provider
- At least one NAA
- POL1, even if not used
- The file system

The Profile structure may contain:

Several Applications (as defined in Global Platform Card Specification) in addition to the MSP-SD
One CASD (as defined in Global Platform Card Specification UICC Configuration)

SECURE CHANNEL ON INTERFACES

Secure Channel on ES5 (SM-SR-eUICC) - The ES5 functions are addressed to the eUICC through a secure channel established between the SM-SR and the ISD-R. The eUICC shall support SCP80 and may support SCP81 (defined in ETSI 102 225 [4] and ETSI 102 226 [5]).
Secure Channel on ES8 (SM-DP - eUICC) - The ES8 functions are addressed to the eUICC through a secure channel established between the SM-DP and its ISD-P. The eUICC shall support SCP03 for ES8 (as defined in Global Platform Card Specification.
Secure Channel on ES6 (MSP-eUICC) - The ES6 functions are addressed to the eUICC through a secure channel (as defined in ETSI TS 102 225 [4] and ETSI TS 102 226 [5]) established between the MSP and the MSP-SD.

SECURITY OVERVIEW

The security requirements have to be applied to the different Actors and Roles (Customer, MSP, SM-DP, SM-SR, CI, eUICC and eUICC Manufacturer, M2M Service Provider). Each Role is considered as elements which can belong to a security realm and has to fulfil the appropriate certification scheme criteria.

- Every SM-SR and SM-DP shall be certified according to a GSMA agreed certification scheme.
- The eUICC shall be certified according to the GSMA eUICC Protection Profile.
- The eUICC Manufacturer shall be SAS certified.
- For the eUICC interfaces, the Platform Management commands (ES5) and the OTA Platform commands (ES6) shall be protected by either a SCP80 or SCP81 secure channel with security level defined in section 2.4. The Profile Management commands (ES8) shall be at least protected by a SCP03 security level

Certificate Issuer

The Certificate Issuer (CI) Role issues the certificates for the eUICC Remote Provisioning System and acts as a trusted third party for the purpose of mutual authentication of the entities of the system.

The CI provides:

- A self-signed Root Certificate used to verify certificates issued and signed by the CI
- A public key (PK.CI.ECDSA), part of that Root Certificate, used on the eUICC to verify certificates issued by the CI
- A certificate (CERT.DP.ECDSA, signed by the CI) to authenticate the SM-DP. This certificate is used in the "Load and Install Profile" procedure
- A certificate (CERT.SR.ECDSA, signed by the CI) to authenticate the SM-SR. This certificate is used in the "SM-SR change" procedure
- A certificate, signed by the CI, to authenticate the EUM. This certificate is used in the "Download and Install Profile" and in the "SM-SR change" procedures.

OTA COMMUNICATION (SM-SR-EUICC)

In the eUICC Remote Provisioning and Management system the OTA communication is exclusively handled by the SM-SR. The SM-SR can use SMS, CAT_TP and HTTPS for remote OTA communication with the eUICC.

2. Physical and logical characteristics

M2M UICC should comply with the specification ETSI TS 102 671 V9.2.0 for following environmental parameters:

- Operational and storage temperature
- Moisture/Reflow conditions
- Humidity
- Corrosion
- Vibration
- Shock
- Memory data retention time
- Minimum updates

This environmental classification system allows each industry sector to specify the target profiles that are appropriate for smart card usage in the automotive environment.

Supported requirements are generally tested by accelerated methodologies that concentrate, over a reduced time period, the constraints that the product is expected to endure during its full intended lifetime. Applicable test specifications for this category are referred to ETSI TS 102 671.

3. Operational and storage temperature

As per TS 102 671 provide test methodologies to assess whether the UICCs are suitable for operation and storage in any of the following temperature ranges:

- -25 °C to +85 °C (standard temperature range)
- -40 °C to +85 °C (class A specific UICC environmental conditions.)
- -40 °C to +105 °C (class B specific UICC environmental conditions)
- -40 °C to +125 °C (class C specific UICC environmental conditions)

TABLE 7 M2M SIM COMPARISON TABLE

	M2M Standard	M2M Class A	M2M Class B	M2M Class C
Temperature range	-25 °C to +85 °C	-40 °C to +85 °C	-40 °C to +105 °C	-40 °C to +125 °C
Lifetime	approx. 5 years	> 10 years	> 10 years	>12 years
Form Factor	2FF, 3FF, MFF1/2	2FF, MFF1/2	MFF1/2	MFF1/2
Segmentation	Tablet PCs, PDAs, Cameras	Metering Systems, Health Care, the Coke Machine	Infotainment, Service, Emergency, Break-down Call	Automobile (Infotainment, Service, Emergency, Break-down Call)
Compliant	ETSI TS 102.221 / MFF1/2 in accordance to ETSI TS 102.671	Fully compliant to 102.671	Additional Process & Quality documentation (e.g. automotive)	Additional Process & Quality documentation (e.g. automotive)

Note: Lifetime describes the combination of min. updates, data retention and an estimation of the usage in the field.

4. Manufacturing and Lifetime Exposure to Humidity

M2M UICCs should support the high humidity condition as specified in TS 102 221 and TS 102 671 provides the following features

- Classification of moisture/ reflow conditions applicable during manufacturing process for soldered UICCs
- Operating conditions under humid environment conditions
- Corrosion in salty atmosphere

5. Shocks and Vibrations

ETSI TS 102 671 allows for the provision of UICCs that meet vibration specification [JESD22Vib] and shock-conditions specifications [JESD22Shk] defined by JEDEC (Joint Electron Device Engineering Council) for automotive applications.

The MFF1/2 UICC form factor specified in ETSI TS 102 671 have been designed to meet the vibrations and shock constraints required for use in automobiles. Besides electrical contact points used for connection they provide large independent mechanical pads intended to solidly anchor them to their hosting circuit board.

6. Lifetime

For any M2M device in automotive environment the average life expectancy is from ten to fifteen years. For the UICC the lifetime not only depends on the data retention and the number of read\write cycles supported by its non-volatile memory (EEPROM or Flash technology), but also on exposure to the environmental constraints, such as storage and operational temperature, humidity

and so on. ETSI TS 102 671 proposes to assess such capabilities by verifying that the UICC information intended for frequent updates support a choice of 100000, 500000 or even 1000000 cycles. This can be combined with a choice of memory retention requirements of 10, 12 or 15 years.

7. Electrical Specification

UICC should comply with MFF1/2 (Machine Form Factor) as defined in ETSI TS 102 671 V9.2.0 and ETSI TS 102 221 with Class C operating condition specified for MFF1/2

8. Device Paring Mechanism

UICC should support following mechanisms for device paring as defined in ETSI TS 102 671

- Secure Channel pairing (Description in ETSI TS 102 484)
- CAT application pairing (Description in ETSI TS 102 223)

The UICC generally remains connected through its serial interface as defined in ETSI TS102 221 only to the modem, which appropriately handles the proactive requests from the card. In an M2M device it could be easy to interface the UICC directly to the application processor in the device. However many of the devices follow the legacy architecture wherein the UICC is connected to the communication module through the serial interface and the module in turn is connected to the application processor of the devise which is based on AT command specification 3GPP TS 27.007.
In M2M devices it will be greatly beneficial if the UICC applications are able to interact with the application processor of the device itself. Hence there is a need to transport toolkit commands through the AT interface with only minimal changes to the AT command set which has been addressed by ETSI SCP by means of changes to TS 102 223 Release 9 allowing it to transport CAT traffic over AT. This enables the UICC to provide a compliment to the functionalities that may be provided by the modem itself.

9. UICC – Device interface

UICC-ME interface should comply with the standards set-out in Table 9

TABLE 8 EUICC STNADARDS

S. No.	Standard Name / Number	Version
1	ETSI TS 101 220 Smart Card ETSI Numbering system for telecommunication application provider	8.4.0
2	ETSI TS 102 221 Smart cards; UICC-Terminal interface; Physical and logical characteristics	8.2.0
3	ETSI TS 102 222Universal Integrated Circuit Cards (UICC); Administrative commands for telecommunications applications	7.0.0
5	ETSI TS 101 116 V7.0.1 (1999-07): Digital cellular telecommunications system (Phase 2+); Specification of the 1.8 Volt Subscriber Identity Module Mobile Equipment (SIM - ME) interface (GSM 11.18 version 7.0.1 Release 1998)	7.0.1
6	3GPP TS 31.101 V5.2.1 (2004-12): 3rd Generation Partnership Project; Technical Specification Group Terminals; UICC-terminal interface; Physical and logical characteristics (Release 5)	5.2.1
7	3GPP TS 31.102 V5.15.0 (2012-09): 3rd Generation Partnership Project;	5.15.0

	Technical Specification Group Core Network and Terminals; Characteristics of the Universal Subscriber Identity Module (USIM) application	

10. UICC Application Tool Kit

The CAT provides mechanisms which allow applications, existing in the UICC, to interact and operate with any terminal which supports the specific mechanism(s) required by the application.

The mechanisms are dependent upon the commands and protocols relevant to CAT as USAT in TS 102 221 for a 3G platform and as SAT in TS 151 011 for a 2G platform.

TABLE 9 UICC STANDARDS

1	ETSI TS 102 221 Smart Cards; UICC-Terminal interface; Physical and logical characteristics	V8.5.0
2	ETSI TS 151 011Smart Cards; Smart Card Platform Requirements Stage 1	V8.4.0

11. OTA capabilities of UICC (Remote file management and Remote Applet management)

It is recommended that the UICC should be in compliance with the ETSI TS 102 225 and ETSI TS 102 226 for standardization and remote management of secure packets/data for following parameters:

- Security system for packets exchange (between an entity in a network and an entity in the UICC.)
- Protocol/structure for generalized secured packets, Response Packet
- Protocol/structure for secured messages based on HTTPS
- Implementation for CAT_TP, TCP/IP
- Remote APDU format
- Security parameters assigned to applications
- Remote File Management (RFM)
- Remote Application Management (RAM)
- Additional command for push
- Confidential application management

TABLE 10 STANDARDS RELATED TO OVER-THE-AIR MANAGEMENT OF THE UICC

1	ETSI TS 102 225 Smart Cards; Secured packet structure for UICC based applications TECHNICAL SPECIFICATION	V8.5.0
2	ETSI TS 102 226 Smart Cards; Remote APDU structure for UICC based applications	V8.3.0

12. Security Requirements

UICC shall be provided with adequate security features to meet basic requirements of confidentiality, integrity, authentication, authorization and preventive actions for potential threats. The security features shall be in conformity with TS 102 689 V2.1.1, TS 102 690.

Remote Subscription Management

13. M2M eUICC Remote Provisioning System

Below diagram specifies the Roles and interfaces associated with the Remote Provisioning and Management of the eUICC, building on GSMA Remote Provisioning Architecture for Embedded UICC.

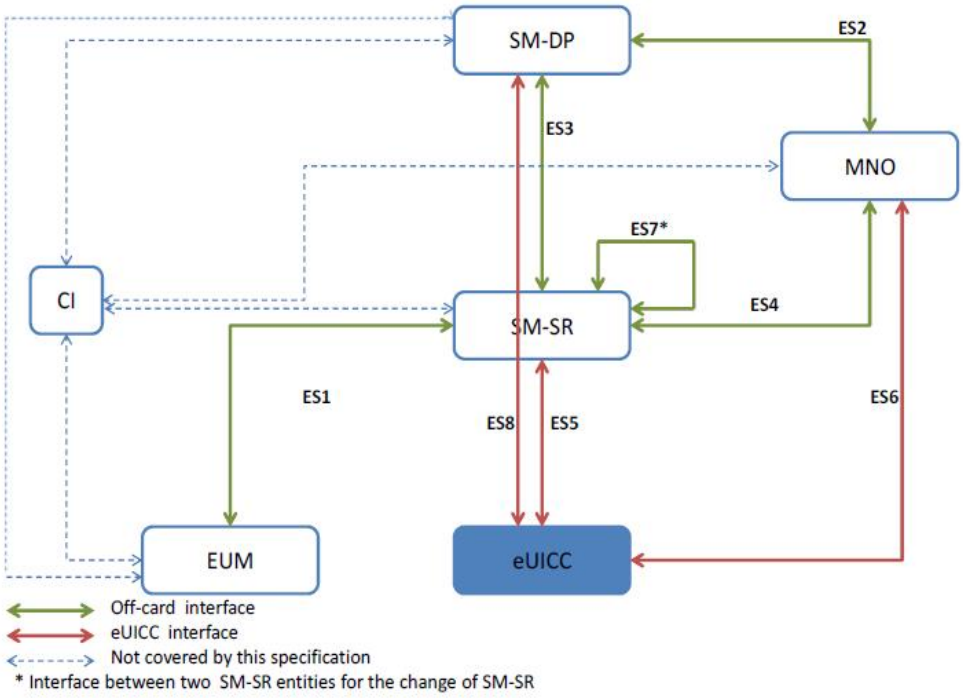


FIGURE 14 EUICC REMOTE PROVISIONING SYSTEM

5 References

1. http://www.transportationissuesdaily.com/webinar-emerging-vehicle-to-vehicle-technology-will-greatly-improve-safety/
2. http://www.iteris.com/cvria/html/applications/app57.html
3. http://www.iteris.com/cvria/html/applications/app11.html
4. 3GPP TSG –SA WG1 Meeting #68 , San Francisco USA November 2014
5. http://www.radio-electronics.com/info/cellulartelecomms/lte-long-term-evolution/4g-lte-advanced-d2d-device-to-device.php
6. http://www.nhai.org/Doc/14jul11/ETC_Specs_June%2020112828319218.pdf

Abbreviations

TABLE 11 ABBREVIATIONS

Abbreviation	Full Name
ARAI	Automotive Research Association of India
AES	Advance Encryption Standard
CDMA	Code Division Multiple Access
CAGR	Compounded Annual Growth Rate
CCTV	Closed Circuit Television
DES	Data Encryption Standard
DIMTS	Delhi Integrated Multi-Modal Transport System
EOBR	Electronic On-Board Recorder
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
GPS	Global Positioning System
HLAP	High Level Application Requirements
IOT	Internet of Things
ITS	Intelligent Transport System
MDS	Minimum Data Set
M2M	Machine to Machine
OBD	On-Board Diagnostics
OTA	Over the Air
RFID	Radio Frequency Identification
RLSVDS	Red Light-Stop Line Violation & Detection System
RSA	Short for the surnames of its designers Ron Rivest, Adi Shamir and Leonard Adleman
SIAM	Society of Indian Automobile Manufacturers
SIM	Subscriber Identification Module
eSIM	embedded SIM – Form Factor of SIM to be soldered into a device at manufacturing
V2V	Vehicle to Vehicle
V2I	Vehicle to Infrastructure

Abbreviation	Full Name
VMS	Variable Message Sign
VTS	Vehicle Tracking System
Wi-Trac	Wireless Traffic Signal Controller
UICC	Universal Integrated Circuit Card – Newest generation of SIM
eUICC	embedded UICC – Form factor of the UICC intended to be soldered into the device during manufacturing.

ISO 9001:2008

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