Question 1 – (Page 61) – Service Authorization Requirements

Whether there is a need to introduce an authorisation for vehicle-to-infrastructure (V2I) communication service under Section 3(1)(a) of the Telecommunications Act, 2023? If yes, please provide input with respect to the following aspects:

(a) Eligibility conditions for the authorisation;

(b) Period of validity of the authorisation and conditions for its renewal;

(c) Service area of the authorisation;

(d) Scope of service of the authorisation;

(e) Technical, operating, security related conditions etc. of the authorisation;

(f) Any other related aspect. Kindly provide a detailed response with justification.

C-DAC Response

C-DAC believes that the V2I communication paradigm is a very important aspect of V2X communication systems, serving several citizen centric needs of road safety and improving traffic efficiency. Most of these services are centered around government driven interventions and target citizen centric use cases becoming a platform for improving road information, safety, and traffic efficiency. Multiple services involving several stakeholders (central, state, municipalities, etc.,) can be provided using V2I. Some of the services that are relevant to governmental use cases for road safety and traffic efficiency include:

- Priority vehicle passage for ambulances, VIP vehicles, etc., through traffic signal control,
- Gantry less and high-speed automated tolling using V2I integrations,
- Road information alerts like diversions, rerouting, blockage, traffic jams, weather information,
- Stranded vehicle alerts for highway safety
- Emergency services during an accident/mishap
- Vehicle tracking services for legal reasons

In our opinion, V2I should be treated as an auxiliary communication service and infrastructure platform that allows governing bodies to disseminate and manage road information and services to the commuting citizen. Therefore, authorization may be essential and should be restricted to Government organizations and their designated trustworthy service providers.

The focus of V2I should be placed on disseminating government-initiated citizen services to the citizen and no other commercial applications. Authorization is important to ensure there is trust in the services and that these are not exploited by malicious actors.

(a) Eligibility Conditions for the Authorization

- All services for V2I should be initiated and maintained under the jurisdiction of Central, State or Governmental Agencies of the country
- Vendors / Service Providers should be Indian organizations
- All devices/equipment and technologies should preferably be designed and developed in the country. In instances where the infrastructure is being sourced from other countries, the vendor should produce a clear Hardware Bill of Material (HBoM) of the products and internal design details for scrutiny.
- Data generated from the transactions should reside in servers within the country and not be sent to other countries.

(b) Period of validity of the authorisation and conditions for its renewal.

Validity of services should be for a period of 5 years with renewal through a quick process, subject to meeting authorization rules as constituted by the Ministry.

(c) Service area of the authorisation

Every V2I use case meets individual service requirements, depending on the particular needs of deployment. For example, priority passing of ambulances and vehicles are state specific issues, under the purview of the traffic police. These may have a very localized service area and may rarely require wider service areas. Similarly, automated toll applications using V2I is restricted to a given geographical boundary upon which the toll exists and is under the purview of MORTH. However, vehicle tracking for legal purposes may come under wider jurisdictions involving multiple state actors. In general, geographic boundaries can be issued depending on the use case.

(d) Scope of service of the authorisation;

The scope is dependent on the services being provided. A suggestion to resolve the scope of the service authorization requirements is to identify potential V2I applications and define their scope. While majority of services shall remain under the ambit of the governing organization and therefore remain localized, some services may require global relevance and therefore, data exchange services may be needed.

(e) Technical, operating, security related conditions etc. of the authorisation.

i. Authorization should be subject to compliance and certification process for the technology
ii. All data that is generated in from the devices should be stored on Indian servers and should be applicable for scrutiny at any point of time.

(f) Any other related aspect. Kindly provide a detailed response with justification.

No Comments

Question 2: Page 62 – Service Authorization

In case your reply to Q1 is no, what should be the mechanism for enabling, facilitating and regulating vehicle-to-infrastructure (V2I) communication service in India? Kindly provide a detailed response with justification.

Not Applicable

Question 3: Page 62 – Service Authorization

Any other suggestions relevant to the authorisation for vehicle-to-infrastructure (V2I) communication service may be submitted with proper explanation and justification.

--

Question 4: Page 65 – Choice of C-V2X Technology

Whether a specific technology (such as LTE-based C-V2X, NR-based C-V2X etc.) should be prescribed for the implementation of C-V2X in India? If yes, which technology should be adopted for the implementation of C-V2X? If no, in what manner, the issues related to inter-operability between different technologies should be addressed? Kindly provide a detailed response with justification.

C-DAC Response

LTE based C-V2X, and NR based C-V2X are complementary technologies that are not designed for interoperability. While NR based C-V2X incorporates broadcast capabilities similar to the LTE based C-V2X specifications, it adds additional capabilities like unicast and groupcast communication. Moreover, LTE based C-V2X systems uses SC-FDMA waveforms for transmissions and targets basic safety and traffic alerts as their primary use cases. NR C-V2X on the other hand is based on CP-OFDM waveforms and targets advanced automotive, autonomous and constrained automotive application requirements. LTE C-V2X supports channel sizes of 10 and 20 MHz, while NR supports upto 40 MHz channels for higher data throughputs. Further, the internal subcarrier spacing in LTE C-V2X remains constant at 15KHz, while NR C-V2X allows 4 numerologies, resulting in variable payload sizes and data rates. This makes these radios fundamentally different in their specifications and implementation aspects and are not designed to interoperate with each other. Therefore, considering a schema for interoperability may not be feasible for all intended functionality and backward compatibility.

Trying to make these two technologies interoperate may require a V2X adaptation layer above the physical hardware, in the higher layers of the communication stack which may add latency to the end-to-end communication. This defeats the requirements of low latency communication for safety related applications. Some approaches that could be proposed include co-existence without horizontal hand-off between the two radios. However, this may be considered in the realm of research. The Bluetooth technology presents this type of architecture, bringing about collaboration between Bluetooth Classic and Bluetooth Low Energy which are physically incompatible with each other, but coexists on the same platform, handing-off based on the target communication requirements.

Given the intent to demonstrate V2V in the next 1 year as mentioned by the Hon. Minister of Road Transport and Highways, the immediate possible solution would be with LTE based C-V2X. This could be considered for a decade with an emphasis on basic safety and traffic alerts as potential use cases. Advanced use cases of autonomous and constrained applications could be considered as Research pilots during this time after which NR V2X which is still being developed and tested, can be matured and thereafter adopted. Cost factor is also an important consideration for V2X.

Question 5: Page 71 – Mandatory Testing and Certification of Telecom Equipment

Whether there is a need to bring road-side units (RSUs) and on-board units (OBUs) under the regime of Mandatory Testing Certification of Telecom Equipment (MTCTE)? If no, in what manner, Electromagnetic Interference (EMI), Electromagnetic Compatibility (EMC), safety, technical and security requirements prescribed by TEC/ DoT may be ensured? Kindly provide a detailed response with justification.

C-DAC Response

A strategy to test and certify OBUs and RSUs is essential. However, several considerations are to be made with regard to OBUs and RSU devices. These are slightly different from normal telecom equipment for the following reasons:

1. These devices if configured to use LTE based C-V2X do not require the telecommunication network because they support sidelink communication that is standalone.
2. These are wireless devices, operating in a specific frequency band and require compliance to operating frequency, power levels, channel usage, data rates, etc. These are essential compliances.
3. However, these devices have communication stacks (IEEE and ETSI specifications) that are standardized and should interoperate with devices manufactured by different vendors. Therefore, communication stack level compliance for interoperability is essential.

4. The standards specify exclusive message formats based on SAE or ETSI standards. All devices are required to comply with these message formats and therefore should be evaluated for such compliance.
5. Cybersecurity is an important consideration in V2X communication. The standards specify PKI based trust hierarchy, communication security and privacy. These require exclusive test compliances.
6. The usage of OBUs and RSUs fall under different sectors/domains like automotive, road infrastructure, traffic signals, etc. There are multiple stake holder ministries and each of these may specify their exclusive compliance requirements for devices under their purview. For example, automotive has a slew of standards and compliances for devices put within vehicles. Similarly, equipment to be deployed in public spaces may require specific consumer grade compliances.
7. All these aspects should be considered as part of the testing and certification processes and requires multi-stakeholder interactions and consultations.
8. Further Key Performance Indicators, Testing Infrastructures, Standards and Use Cases have to be built and scaled for the needs of the country.
9. An approach involving multiple organizations like TEC, ARAI, GARC, ICAT and other relevant testing organizations should brainstorm and come up with a unified process and testing scheme. C-DAC and MeitY which has been involved in the development of this technology will surely support the technical requirements for such activity.
10. A pilot project to this effect is essential for the country.

Question 6: Page 80 – Higher Layer Communication Stack Considerations

To ensure inter-operability among different RSUs/ OBUs, whether there is a need to standardize the layered communication framework (stack) for higher layers (other than the access layer in which C-V2X will be used) of Intelligent Transportation System (ITS)? If yes, which standard for ITS stack and security should be adopted? Specifically, whether the ETSI standard for ITS stack and security, as recommended by the Task Force on Intelligent Transportation System for the use of 5.9 GHz (mentioned at para 3.5 of this consultation paper) should be adopted? If no, in what manner, inter-operability among different RSUs/ OBUs can be ensured? Kindly provide a detailed response with justification.

C-DAC Response

1. Yes, there is a need to standardize higher layers of the V2X stack for interoperability within the country.
2. In our understanding, the IEEE 1609.x stack is simple to understand and easy to implement but targets a specific set of use cases. The ETSI stack on the other hand has multiple parts and is more scalable, covering wider use cases for futuristic applications. For example, at the network layer, the IEEE stack specifies the WAVE protocol which is typically a single-hop broadcast specification, targeting the local geographical region around the vehicle. It does not consider larger multi-hop use cases in the vehicular network. On the other hand, in the ETSI stack, the network layer is specified by a standard called Geo-Networking which has multiple parts and is scalable supporting single-hop broadcast and multi-hop communication schemes. It specifies different paradigms of network communication in which the event/incident geographical area could be connected through another network area via multihop communication of packets. This allows futuristic applications to be developed using the standard.
3. At the transport layer, the IEEE stack does not specify any particular function for the transport layer but only allocates a bit in the header for its presence. ETSI however defines ports that are connected to specific application use cases.

4. Concerning the security layer, the ETSI stack refers to the IEEE stack and modifies a few of its specifications for European use cases. While the certificate format of ETSI uses the IEEE 1609.2 format, there are some differences in the architecture of the PKI model and the trust hierarchies.
5. In our understanding, ETSI stack provides wider coverage with better features and should be adopted as the India stack for the country.

Question 7: Page 80 and 81 - Security Framework for ITS/C-V2X in India

Whether there is a need for prescribing a security framework for ITS/ C-V2X in India? If yes,

(a) What should be the security framework for ITS/ C-V2X?

(b) Which agency [such as Controller of Certifying Authorities (CCA), Ministry of Electronics & Information Technology (MeitY)] should implement the Public Key Infrastructure (PKI) framework for ITS/ C-V2X in India?

(c) How to ensure coexistence of V2X PKI certificates with the legacy PKI mechanism in India i.e. based on X.509, operated by Root Certifying Authority of India (RCAI)?

C-DAC Response

Yes, there is a need for prescribing an indigenous security framework for ITS/C-V2X in India. We should have our own national policy that defines the security architecture of ITS/C-V2X implementations in the country. This is specifically important because the advent and induction of V2X technologies makes the vehicular ecosystem and its supporting devices and technologies a new critical infrastructure. This opens up a new set of attack surfaces, which are different earlier physical attacks on the vehicular system. From the national perspective, it is pertinent to adopt a unified plan and not a siloed approach in establishing security frameworks of different domains and their corresponding security requirements because cybersecurity requires a niche skillset which may not be available with other system/domains. This may lead to dependence on external arrangements and solutions which may result in gaps/incomplete coverage.

(a) What should be the security framework for ITS/ C-V2X?

The ETSI and IEEE standards specify security requirements and the associated security architecture that brings about security, trust and privacy, while ensuring interoperability between different system components defined in the ITS/C-V2X network i.e., OBUs and RSUs. These devices and technologies are typically developed by different manufacturers/vendors, therefore trust and interoperability are essential. At the heart of the security architecture is a PKI based trust model which is grounded on a unique format of the digital certificate that is specified in the IEEE 1609.2 standard. This certificate incorporates policies and requirements that are native to ITS/C-V2X needs. One aspect of its uniqueness is in the inclusion of authorization permissions for different types of ITS use cases, within the certificate. This enables a low latency and trustable service discovery feature that allows devices in the network to choose whether or not they would like to engage with other devices for communication. The certificate itself is different from traditional IETF specified X.509 certificates that which used in may PKI based trust models like web applications, document signing, email clients, etc.

While adopting a standards compliant framework for interoperability is essential, what is additionally required is to build a system that is compatible with existing regulations of the Country. In India, the use of digital certificates as a legal form of authentication is emphasized in the IT act. The Controller for Certifying Authorities (CCA) under MeitY is a statutory body responsible for the implementation of Digital Certificates in the country. The CCA has implemented the Root CA of India (RCAI) which is an entity, responsible to sign digital certificates of CA services providers in the country. The trust model is a centralized hierarchy with the chain of trust resting with RCAI. The RCAI proposes the use of X.509

certificates in the country. However, the ITS/C-V2X standards specifies the IEEE 1609.2 ITS certificate format as its accepted format. Rather than creating a silo of different trust hierarchies, it is proposed to develop a bridge network for coexistence of both certificate formats, thereby bringing the ITS/C-V2X certificates under the trust chain of the RCAI. This methodology ensures compatibility with the existing RCAI trust model, while ensuring interoperability at the device level with global standards.

(b) Which agency [such as Controller of Certifying Authorities (CCA), Ministry of Electronics & Information Technology (MeitY)] should implement the Public Key Infrastructure (PKI) framework for ITS/ C-V2X in India?

In the national context, CCA is the best suited organization to implement the PKI framework for ITS/C-V2X in the country. CCA has already established the RCAI which is the trust anchor for web application, document signing and email transactions in the country. The same technology could be extended to support the PKI architecture as specified by ITS/C-V2X requirements in the country.

(c) How to ensure coexistence of V2X PKI certificates with the legacy PKI mechanism in India i.e. based on X.509, operated by Root Certifying Authority of India (RCAI)?

CCA has implemented a pilot project to demonstrate ITS/C-V2X certificate coexistence. The project was implemented by C-DAC Hyderabad which is a scientific society of MeitY. The technology developed by C-DAC ensures a standards compliant implementation of certificate co-existence through the counter signing scheme specified in RFC 5652 - Cryptographic Message Syntax (CMS) standard. The project also ensures ITS standards compliance (with IEEE and ETSI standards) bringing about interoperability between different ITS/C-V2X devices in the network. The co-existence framework does not require any change in the ITS/C-V2X implementation, especially at the device level. However, there are minimal changes that are required on CA software to ensure compliance and validation on the RCAI trust chain.

Two new components are specified in the security architecture known as the Bharat Automotive CA (BACA) which is the bridge CA between RCAI and the ITS security framework and therefore implements the co-existence framework through counter signing scheme, and the Bharat Automotive Trust List Manager (BATLM) which maintains the certificate trust list for the V2X network. All other components of the ITS/C-V2X security architecture/framework remain the same.

Question 8: Page 101 – Spectrum Allocation

What should be the regulatory framework for the assignment of frequency spectrum to the entities holding the proposed V2I communication service authorisation? Specifically,

(a) Whether there is a need for partitioning the 30 MHz spectrum (5,875-5,905 MHz) for specific applications such as “safety applications” and “operational applications (non-safety applications)”?

C-DAC Response

It may be a good idea to partition the spectrum into 2 parts for safety and non-safety applications. Other countries have specified the same with the flexibility of merging as per use case. For safety applications, a spectrum allocation of 10MHz may be sufficient. The remaining 20 MHz could be allocated to non-safety applications.

While partitioning of spectrum may be a good idea, whether this could be implemented and is practically feasible remains to be seen. Existing C-V2X lower layer standards do not specify channel switching. In earlier DSRC systems, the standards specified switching between one control channel and 6 service channels, every 50 milli seconds. This meant every device would listen on the control channel for 50 milli seconds and switch to a service channel of interest, based on the services provided in that zone/area. However, in LTE based C-V2X systems, lower layers do not specify any

mechanism of switching between the channels. The implication of partitioning the spectrum may require one of the following approaches to be considered:

- Develop a channel switching protocol at the MAC layer which allows the device radio to switch periodically between the two channel definitions. This would however make the implementation globally incompatible with standards and practices.
- Use 2 radios on a device, centered on the 2 channels to simultaneously receive both transmissions. However, this would increase cost.

A deeper discussion on this matter is required to deal with the above aspects. However, it may be good to specify spectrum partitioning, because this will provide flexibility in the future to configure and resuse spectrum as per the use case requirements and needs.

(b) In case more than one authorised entity has to operate in the same geographical area, what should be the mechanism for simultaneous use of the spectrum? Specifically, whether the spectrum should be divided amongst the authorised entities in an exclusive manner, or should the authorised entities utilize the spectrum in a shared manner?

The radio layer of LTE based C-V2X devices allows simultaneous access of the channel by multiple devices. Therefore, more than one authorised entity is allowed to operate and coexist in the same geographical area, simultaneously using sub channel and sub frame selections, autonomously.

LTE based C-V2X radios use a technology called Single Carrier FDMA (SC-FDMA) for channel access and supports 2 typical channel bandwidths - 10 MHz and 20 MHz. The channel is divided into 180 KHz Resource Blocks (RB). Each RB is composed of 12 sub carriers of 15 KHz each. Multiple RBs are grouped together to form a sub-channel. The number of RBs that compose a sub-channel is pre-configured either by the basestation (eNodeB or gNodeB) dynamically or predefined/default (in out of network use cases). Multiple sub-channels are created to consume the available bandwidth. Sub-channels are used to transmit data and control information.

In LTE based C-V2X, channels are organized as 1ms subframes in the time domain. Each subframe has 14 OFDM symbols with normal cyclic prefix. 9 of these symbols are used to transmit data, 4 are used as demodulation reference signals and 1 is used as a guard symbol. The guard symbol is important for timing adjustments (sync) and switching between tx and rx across subframes. A sub-channel includes RBs in the same subframe.

Data contained in a sub-channel is organized in a Transport Block (TB) that is carried in a physical sidelink shared channel (PSSCH). A TB holds a full packet (BSM, CAM, etc). A TB can occupy several sub-channels depending on (i) size of the packet, (ii) Pre-Configuration of no of RBs in a sub-channel and (iii) Modulation Scheme.

LTE based C-V2X systems uses a sensing based Semi-Persistent Scheduling (SPS) scheme for resource allocation of the available channel. This conforms to mode 4 of the resource allocation modes. In this scheme, devices sense the channel for a predefined duration of time to identify sub-channels in sub-frames that are free. They choose their sub-channels and announce their selection to other devices, indicating corresponding subframes in which they will transmit, based on the periodicity of their transmissions. Therefore, devices can autonomously choose their transmit channels and indicate the same to other devices, operating in the same geographical area in which the service persists.

In this context, more than one authorized entity can co-exist in the same geographical area, sharing the available spectrum and providing specific services to other devices, without requiring any specific allocation. The spectrum does not earmark any exclusive channels for any particular service or authorized entity and all have to contend for the spectrum using the SPS scheme.

(c) If your response to part (b) is "in an exclusive manner", what should be the minimum quantity of spectrum to be assigned to each entity holding the proposed V2I communication

service authorisation? If your response to part (b) is "in a shared manner", whether there is a need to prescribe a mechanism for interference management?

The sensing based SPS scheme described in the above section manages spectrum usage amidst contending devices in the same geographical area, avoiding interference or collisions. The PHY and MAC layer protocols specify techniques through which collisions and interference could be avoided in the spectrum usage. However, congestion is a challenge and it is important to establish the extent and bounds beyond which communication degrades in the network. Congestion control techniques and anti-jamming techniques should be investigated to protect the network from unwarranted situations.

(d) For interference management, whether there is a need to prescribe –
- **(i) minimum directionality of road-side unit (RSU), or**
- **(ii) protection distance between the RSUs, or**
- **(iii) maximum antenna height for RSUs? If yes, what should be such parameter(s)?**

The LTE based C-V2X radio is essentially a broadcast network. Every device in the network, whether an OBU or RSU contends for the spectrum usage at the same time and chooses its subchannel in which it intends to transmit. Alternatively, these devices remain in always receive mode and receive packets that are transmitted by every other device in the geographical area or within its range. The typical range of a C-V2X radio is about 1 km, line-of-sight and omni-directional.

Prescribing the directionality, antenna height, and protection distances, allows us to restrict or expand the coverage area of intended services. This depends on the use case. For example, traffic signal monitoring and emergency vehicle passing may require to be restricted to a geo-fenced geographical area, relevant a limited range of service provision, while toll management or highway alerts may require extended coverage. By configuring directionality and maximum antenna height, these aspects can be established, according to the need of the use case.

In USA, FCC prescribes the antenna height for an RSU to be within the range of 8 to 15 meters. FCC has adopted an EIRP PSD limit for RSUs without limiting the maximum transmitted power output. The PSD limit ensures that transmitters are restricted in their overall EIRP since it maintains the limit over the entire allocated bandwidth. The FCC adopts 33 dBm/10MHz, 33dBm/20MHz and 33/30MHz as the maximum radiated power allowed for RSUs. At the height of 8 meters, RSUs are allowed to broadcast at maximum power, but the power has to proportionally reduce as the height increases upto 15 meters.

In order to maintain segregation between authorized service providers, it may be good to prescribe a protection distance of 2kms between RSUs. However, this prescription depends on the specific use case and may be more relevant to highway applications and not urban and city wide use cases.

(e) Whether there is need to mandate a mechanism for obtaining prior approval (analogous to SACFA clearance) for the establishment of RSUs by the entities holding the proposed V2I communication service authorisation? If no, in what manner, the establishment of RSUs should be regulated?

Yes, a mechanism of prior approval and authorisation is essential for establishment of RSUs. While aspects pertaining to SACFA clearance are important, other aspects which also need to be considered are: Radiating power, Deployment height, Channel usage, Communication Stack Compliance, Interoperability, Application Message Compliance, etc. An appropriate testing lab with standardized test cases and testing requirements should be established to ensure that all devices access the spectrum and communicate homgenously in the network.

(f) For avoiding (i) interference between RSUs, (ii) interference between RSUs and OBUs, and (iii) interference between OBUs, whether the radiated power limits for OBUs and RSUs and OOBE limits, recommended by the Task Force on Intelligent Transportation System for the

use of 5.9 GHz (mentioned at para 3.4 of this consultation paper) should be adopted? If no, what should be the radiated power limits for OBUs and RSUs and OOBE limits?

The task force on ITS has recommended 4W EIRP transmitter power output for both OBUs and RSUs and a conducted output power of 23 dBm (200 mw) over 20 MHz spectrum for RSUs. Pertaining to the same, C-DAC expresses its reservations. C-DAC suggests that India adopts PSD EIRP limits and restricts the OBU PSD to 23 dBm over all bandwidth allocations, 10 MHz, 20 MHz, 30 MHz. Similarly, the PSD EIRP for RSUs should be set to 36 dBM and height should be restricted to 10 meters. OOBE limits

(g) What should be the maximum period of assignment of spectrum to the entities holding the proposed V2I communication service authorisation?

A duration of 5 years may be proposed for the initial assignment of spectrum following which a reassessment may be made.

(h) Whether there is a need to prescribe roll-out obligations associated with the assignment of spectrum to the entities holding the proposed V2I communication service authorisation?

There may be need for compliance and certification obligations for entities holding V2I service authorizations.

(i) Whether there is a need to introduce a provision for the surrender of frequency spectrum? Kindly provide a detailed response with justification.

In the current context of the technology, the provision to surrender frequency spectrum comes after review of how the technology is being used and integrated in the system.

Question 9: Timeline for Processing Spectrum Assignment Application

Whether there is a need for prescribing timelines for processing the applications for the assignment of spectrum to the entities holding the proposed V2I communication service authorisation? Kindly provide a detailed response with justification.

No comments

Question 10:

Whether there are any other suggestions related to assignment of spectrum to the entities holding the proposed V2I communication service authorisation? Please provide a detailed response with justification.

No comments

Question 11.

Any other issues/ suggestions relevant to the regulatory framework for V2X communication may be submitted with proper explanation and justification.

C-DAC Response

1. Establishing a clear set of standards pertaining to the radio interface, communication stack and message layer formats is important.
2. Identifying use cases which are relevant to the Indian context and defining unique message formats and standards for these messages is important
3. Developing pilot implementations in the country to test and verify the use of this technology is important, before wide scale adoption and roll out

4. Developing infrastructure, testing tools and testing standards and proliferating the same for equitable performance evaluation across multiple vendors and stakeholders is essential
5. Having adoption via regulation is essential in the V2X environment. However, such regulation should be entertained only after thorough inspection and field testing of the technology.
6. The spectrum may be provided for the immediate 5 years as a stage for testing and establishing the technology and building India centric use cases which are pertinent and essential to road safety.

Question 12.

In view of the public welfare-oriented nature of V2X applications and the need to encourage the deployment of such infrastructure and services, should there be spectrum charges levied on spectrum assigned to the V2I communication service authorised entities under the proposed V2I communication service authorisation? Please provide detailed justification in support of your response.

C-DAC Response

1. The levy of spectrum charges is a state specific issue and should be considered according to procedures and processes of the country. It may be pertinent to note that every other nation does not levy charges to the spectrum usage in view of public safety and welfare considerations.
2. With regard to the technology, both OBU and RSUs use the same spectrum and there is no difference between either device with respect to the radio access layer. Therefore, whether such a spectrum charge can be levied only on RSU services should be discussed and applied. The spectrum usage models applicable to mobile communication may also be considered in this context. However, since V2X is predominantly related to road safety and public information services, exceptions may be considered in the interest of public good.
3. From the perspective of use cases, both V2V and V2I present safety and non-safety application usages. Collision Avoidance, Emergency Braking, Wrong Way Driving are classic examples of road safety applications in the V2V paradigm, while Intersection Warnings, Stranded Vehicle Alerts, etc., present equally important road safety use cases that are based on the V2I paradigm. Another important consideration for V2I is its support for public information services like Road Repair Alerts, Emergency Services, Traffic Management and Signals and Gantry Less Toll Management applications. These provide services for public good and are very important use cases enabling user engagement.

Question 13:

If answer to Q12 is affirmative, whether the spectrum charges for the V2I communication service authorised entities under the proposed V2I communication service authorisation should be determined based on the spectrum charging methodology prescribed by the Department of Telecommunications (DoT) vide its order dated 11.12.2023? If yes, then which of the radiocommunication services specified in the said order, should be taken as basis for calculation of spectrum Charges? Please provide detailed justification in support of your response.

No Comments

Question 14:

If answer to Q12 is affirmative, whether the spectrum charges for the V2I communication service authorised entities under the proposed V2I communication service authorisation should be levied as a percentage of Adjusted Gross Revenue (AGR)? If yes, are there any specific operational/ non-operational revenue items that should be included in/ excluded from AGR for the purpose of determination of spectrum charges? Please provide your response with detailed justification.

No Comments

Question 15:

If response to questions 13 and 14 is negative, then what should be the appropriate methodology for determination of spectrum charges for the V2I communication service authorised entities under the proposed V2I communication service authorisation? Please provide detailed justification in support of your response.

C-DAC Response

In our opinion, spectrum charges should be treated equally between V2V and V2I use cases and should not be differentiated. However, C-DAC would suggest waiving off spectrum charges until the period of technology prototyping and testing is completed.

Question 16

For spectrum assigned to the V2I communication service authorised entities under the proposed V2I communication service authorisation, what should be the appropriate payment terms for spectrum charges, if any? Please provide your response with detailed justification.

No Comments

Question 17

What are the potential sources of revenue, if any, for an V2I communication service authorised entity under the proposed V2I communication service authorisation? Please provide your response with detailed justification.

C-DAC Response

1. Depending on the use case or application service, the sources of revenue may vary.
2. For example, for traffic signals, there may not be any possibility of revenue generation. Traffic signals being a public utility, the additional cost of the RSU and its interface adapter may have to be borne by the corresponding authority that implements the public welfare utility. Since Emergency Vehicle Passage and Signal Phase and Timing (SPAT) messages are essentially meant for public good, building a revenue model around them may not be feasible.
3. In the case of gantry less toll management, the RSU infrastructure could earn revenue through toll charges by appropriating a small part of it for the technology charges.
4. Similarly, highway RSUs that provide alerts and other services could earn revenue through advertising services, which could be a lucrative means of billing the products. However, these may have to be issued under non-safety applications and should be regulated so that public welfare gets priority over other applications.

Question 18

What should be the definitions of Gross Revenue (GR), Applicable Gross Revenue (ApGR), and Adjusted Gross Revenue (AGR) for V2I communication service authorised entity under the proposed V2I communication service authorisation? Further, what should be the relevant items of revenue, exclusions and deductions and consequent definitions of GR, AGR and ApGR? Please provide your response with detailed justification.

No Comments

Q19. What revenue components should be included in, or excluded from, the computation of Gross Revenue (GR), Applicable Gross Revenue (ApGR) and Adjusted Gross Revenue (AGR) for the purpose of determining authorisation fees or spectrum charges for the proposed V2I communication service authorisation? Please provide your response with detailed justification.

No Comments

Q20. Whether revenue derived from safety-related V2X services under the proposed V2I communication service authorisation should be excluded from the computation of AGR, in view of their public interest and non-commercial nature? Please provide your response with detailed justification.

No comments

Q21. What should be the appropriate entry fee for V2I communication service authorised entities under the proposed V2I communication service authorisation? Please provide detailed justification in support of your response.

No Comments

Q22. What should be the appropriate terms and conditions for bank guarantees for the proposed V2I communication service authorisation? Please provide detailed justification in support of your response.

No Comments

Q23. What should be the applicable minimum equity and minimum net worth requirements for authorised entities under the proposed V2I communication service authorisation? Please provide detailed justification in support of your response.

No Comments

Q24. What should be the applicable application processing fee for the proposed V2I communication service authorisation? Please provide detailed justification in support of your response.

No Comments

Q25. What should be the applicable rate of authorisation fee for proposed V2I communication service authorisation? Please provide detailed justification in support of your response.

No Comments

Q26. Apart from the financial provisions discussed earlier, are there any other financial terms and conditions that should be made applicable for the proposed V2I communication service authorisation? Please provide detailed justification in support of your response.

No Comments