Ambimat Technologies Pvt Ltd
(A part of the Ambimat Group of Companies)
Ahmedabad, Gujarat, India

May 2026

FORMAL STAKEHOLDER RESPONSE

Response to TRAI Consultation Paper on V2X Communication

Chapter V: Issues for Consultation (Pages 135–142)
CP No. 30/04/2026

Submitted in response to the Telecom Regulatory Authority of India's Consultation Paper on Regulatory Framework for Vehicle-to-Everything (V2X) Communication, released 30 April 2026.

Submitting Organisation

Ambimat Technologies Pvt Ltd
(A part of the Ambimat Group of Companies)
Ahmedabad, Gujarat 380015, India

Contact Person: Neel Shah
neel.shah@ambimat.com
+91 99799 33498

Classification: Public
Version: 1.0
Date: May 2026

0 Contents

0 Executive Summary

This document constitutes Ambimat Technologies Pvt Ltd's formal stakeholder response to TRAI's Consultation Paper on V2X Communication (CP 30/04/2026), Chapter V.

Ambimat Technologies Pvt Ltd is an embedded systems and hardware security engineering company established in 1981, Ahmedabad. Through its AmbiSecure business unit, the company develops hardware-backed identity systems, cryptographic provisioning infrastructure, JavaCard applets, secure element integrations, FIDO2 authenticators, PKI tooling, and IoT trust architectures — capabilities directly relevant to the security and trust infrastructure questions in this consultation.

1. **V2I authorisation is necessary.** A dedicated authorisation under Section 3(1)(a) of the Telecommunications Act, 2023 is appropriate and will provide regulatory clarity for responsible deployment.
2. **Technology: NR-C-V2X as the primary standard**, with LTE-C-V2X permitted as a transitional path. Prescribing only LTE risks locking infrastructure to an earlier generation.
3. **MTCTE for RSUs and OBUs is essential.** These are active endpoints in a public safety cryptographic trust chain. Mandatory testing is the minimum appropriate governance baseline.
4. **A dedicated V2X PKI framework is the most critical single decision in this consultation.** Without it, all other technical investments are vulnerable.
5. **Safety-spectrum charges should be waived or nominal.** V2X safety applications are public welfare infrastructure, not commercial services.
6. **Domestic manufacturing capability** in security-critical V2X components should be encouraged through authorisation conditions.

1 Authorisation Framework for V2I Communication (Q1–Q3)

1.1 Q1: Need for V2I Authorisation Under Section 3(1)(a)

Whether there is a need to introduce an authorisation for V2I communication service under Section 3(1)(a) of the Telecommunications Act, 2023?

Response: Yes. A dedicated V2I communication service authorisation is necessary.

V2I communication is a distinct telecommunications activity: it involves the broadcast and receipt of structured, safety-critical messages between road infrastructure nodes (RSUs) and mobile endpoints (OBUs) over licensed radio spectrum. This activity does not fit cleanly within any existing authorisation category and requires a specific regulatory instrument to define accountability, security obligations, and compliance expectations.

Aspects of the Authorisation:

(a) Eligibility conditions. Applicants should demonstrate: technical capability to deploy and operate RSU infrastructure; financial capacity commensurate with deployment scale; organisational capacity to implement cybersecurity requirements including certificate lifecycle management and incident response; compliance with TEC/DoT technical standards; and no prior disqualification under telecommunications law.

(b) Period of validity. An initial 10-year authorisation, renewable for 5-year periods, is recommended. Renewal should be conditional on demonstrated compliance with updated security and technical requirements.

(c) Service area. National in scope, with geographic deployment notifications required. This supports interference management, emergency coordination, and security audit.

(d) Scope of service. The authorisation should cover: operation of RSU infrastructure on the 5.9 GHz band; broadcast and relay of V2I/V2V/V2P messages; management of PKI certificates for RSU identity and message signing; collection and transmission of road-state data; and over-the-air management of RSU firmware and configuration. The authorisation should explicitly *not* extend to general commercial telecommunications or collection of personally identifiable location data beyond operational necessity.

(e) Technical, operating, security conditions. RSUs and OBUs must carry valid V2X PKI certificates at all times; all V2X message broadcasts must be cryptographically signed; firmware must be updated only through authenticated, integrity-verified channels; RSUs must implement tamper detection; and security incidents must be reported to CERT-In within mandated timeframes.

1.2 Q2: Alternative Mechanism (Not Applicable)

Response to Q1 is affirmative. Q2 is not applicable.

1.3 Q3: Additional Suggestions on V2I Authorisation

1. **Domestic manufacturing incentive.** Authorisation conditions should encourage use of MTCTE-certified and, where feasible, domestically designed and manufactured V2X equipment. This reduces strategic dependency on imported infrastructure carrying road safety data at national scale.

2. **Interoperability testing.** Beyond individual MTCTE equipment certification, a system-level interoperability testing programme RSU-OBU interworking at the V2X application layer should be established separately from but complementary to MTCTE.

3. **Phased deployment obligations.** Initial pilot on defined corridors (e.g., National Highways), followed by mandatory expansion milestones. This allows the device and infrastructure ecosystem time to mature.

4. **Liability framework.** The authorisation must address liability for safety-critical V2X message failures from equipment malfunction, PKI revocation latency, or deliberate message injection. This is particularly important because V2X messages may directly influence autonomous or driver- assist vehicle behaviour.

2 Technology Standards (Q4)

2.1 Q4: Technology Prescription for C-V2X

Whether a specific technology should be prescribed for C-V2X in India?

Response: Prescribe NR-based C-V2X as the primary standard, with LTE-based C-V2X permitted as a transitional technology.

Technology	Strengths	Limitations
LTE-C-V2X (PC5 Mode 4)	Commercially deployed; no network required for PC5; mature chipsets	Not designed for Level 4/5 autonomy latency requirements; legacy path
NR-C-V2X (Release 16+)	Designed for autonomous vehicle requirements; 5G ecosystem alignment; PC5 + Uu modes	Nascent deployment experience; growing chipset availability
DSRC (IEEE 802.11p)	Mature in US/EU; established standards	Being phased out globally; not recommended for India

Recommended approach:

1. Designate NR-based C-V2X as the mandated technology for all new infrastructure after a defined effective date (recommend: 18 months post- authorisation framework publication).

2. Permit LTE-based C-V2X deployments for an initial transitional period (recommend: 5 years from authorisation).

3. Mandate dual-mode capability (LTE + NR) for RSUs deployed after the effective date, to maintain backward compatibility with the installed OBU base.

India's automotive OEM ecosystem is in early-stage V2X planning. A clear NR-V2X mandate aligned with global OEM roadmaps avoids the risk of creating a fragmented domestic market. A defined transition window accommodates near-term LTE-C-V2X equipment availability.

3 Equipment Certification and Standards (Q5–Q6)

3.1 Q5: RSUs and OBUs under MTCTE

Whether RSUs and OBUs should be brought under MTCTE?

Response: Yes. MTCTE coverage is both necessary and proportionate.

RSUs and OBUs are not passive radio devices. They are:

- Active endpoints in a cryptographic trust chain, holding identity certificates and signing every V2X message they originate;
- Connected to the V2X PKI for certificate lifecycle management;
- Capable of influencing driver and autonomous vehicle behaviour through the messages they broadcast;
- Deployed at scale in public locations with limited physical security.

A compromised RSU can broadcast false road-state information across an entire intersection. A miscertified OBU can inject spoofed messages into a vehicle's safety system.

MTCTE scope for V2X equipment should cover:

1. **RF conformance:** Compliance with 5.9 GHz band parameters, OOBE limits, and channel access procedures;
2. **EMI/EMC:** Standard electromagnetic compatibility testing;
3. **Cybersecurity baseline:** This is the most critical and least established aspect. MTCTE should incorporate security requirements aligned with: TEC 31318:2021 (IoT Security); V2X PKI certificate management requirements; secure boot and authenticated firmware update requirements; and *hardware-backed key storage* (V2X identity keys must reside in a hardware-isolated secure element, not in software);
4. **Protocol conformance:** Compliance with the mandated ITS stack.

3.1.1 Hardware Root of Trust: A Mandatory Cybersecurity Baseline

Every RSU and OBU deployed in India's V2X infrastructure should incorporate a dedicated hardware secure element functioning as a hardware root of trust. This requirement is not discretionary: V2X message integrity and device identity assurance cannot be reliably achieved through software-only implementations in open, field-deployed environments subject to physical access and firmware tampering.

The secure element should, at minimum, satisfy a recognised tamper-resistance evaluation profile Common Criteria EAL5+ or equivalent and provide the following capabilities as hardware-enforced functions:

- **Secure key generation and injection:** Private keys for enrolment credentials and pseudonymous certificates must be generated within, or injected under cryptographic protection into, the secure element. No plaintext private key material should exist outside the hardware boundary.
- **Cryptographic signing and verification:** Every outbound V2X message must be signed using a key held within the secure element. Every inbound V2X message must be signature-verified against PKI-backed trust anchors before the host system acts upon its content.
- **Hardware-isolated cryptographic execution:** Sign, verify, encrypt, decrypt, and key-agreement operations must execute within the tamper-resistant boundary, not in host MCU firmware.
- **Certificate lifecycle management:** The secure element should manage enrolment credential storage, pseudonymous certificate receipt and rotation, and certificate expiry tracking, in a manner consistent with the EA/AA architecture described in Section 4.
- **Anti-cloning and attestation:** The device must be provably unique. The secure element must support hardware attestation a signed assertion of device identity derivable from a root key that cannot be extracted or replicated.
- **Tamper resistance and lifecycle trust:** Active tamper detection, secure boot chain validation, and integrity-locked firmware update authorisation must all be enforced at the hardware level, not solely in firmware.

These requirements apply across the full scope of V2X trust operations: V2X message signing and verification, firmware validation, credential protection, enrolment credential custody, pseudonymous certificate management, and trust chain validation up to the V2X Root CA.

Implementation approaches may include dedicated hardware trust modules designed for embedded cryptographic identity, secure key storage, PKI-backed authentication, signing, attestation, and secure lifecycle management. The AmbiSEC secure identity platform represents one such reference architecture: an embedded co-processor providing hardware-backed PKI operations, secure key lifecycle management, and cryptographic trust enforcement in a form factor suited to OBU and RSU integration. Such platforms have been deployed in city-scale IoT and infrastructure programmes outside India, demonstrating operational viability at deployment scale.

TEC should explicitly reference hardware root of trust requirements specifying minimum tamper-resistance evaluation levels and mandatory cryptographic function scope in the V2X-specific MTCTE test specifications recommended in the preceding section.

Recommendation

TEC should publish V2X-specific MTCTE test specifications, aligned with ETSI TS 102 941 and ETSI TS 103 097, through a public consultative process before mandating compliance. Establishing NABL-accredited test laboratories with V2X competence will be required.

3.2 Q6: Standardisation of ITS Communication Stack

Whether there is a need to standardise the ITS communication stack for higher layers?

Response: Yes. Adoption of ETSI ITS standards is strongly recommended for the higher communication layers.

Without standardised higher layers, V2X-equipped vehicles cannot exchange meaningful safety information with RSUs from different manufacturers, even on the same C-V2X radio platform. The ETSI ITS protocol stack is the most mature and widely-adopted framework for this purpose:

Layer	ETSI Standard	Function
Application	EN 302 637-2/3	CAM / DENM message formats
Facilities	EN 302 636	Service management, addressing
Network / Transport	EN 302 636-4	BTP, GeoNetworking
Security	**ETSI TS 103 097**	Message signing, certificate formats
Access	LTE-PC5 / NR-PC5	C-V2X radio

Adaptation for India: The ETSI security framework includes a European trust anchor (ECIES). India should establish its own V2X Root CA while retaining the ETSI TS 103 097 message format standard. The certificate format can remain ETSI-aligned while the trust hierarchy is national.

Role of the Office of the Controller of Certifying Authorities (CCA): India's existing digital trust infrastructure provides a natural institutional foundation for V2X PKI governance. The Office of the Controller of Certifying Authorities (CCA), established under the Information Technology Act, 2000, and currently responsible for licensing and regulating Certifying Authorities in India, is well-positioned to assume a central governance role in India's V2X trust hierarchy.

Specifically, the CCA should be considered for the following functions within the V2X trust architecture:

- **V2X Root CA governance:** Exercising statutory oversight of the national V2X Root CA, consistent with the CCA's existing role as the apex authority over India's PKI ecosystem under the IT Act framework;
- **Trust hierarchy management:** Defining the certificate policy and certification practice statement (CP/CPS) framework governing the relationships between the V2X Root CA, Enrolment Authorities, and Authorisation Authorities;
- **PKI oversight and audit:** Conducting or commissioning periodic audits of V2X PKI operations, consistent with the CCA's audit functions over licensed Certifying Authorities;
- **Certificate governance:** Establishing certificate profiles, validity periods, and key usage constraints for V2X enrolment credentials and pseudonymous certificates, aligned with ETSI TS 103 097 and IEEE 1609.2 structural requirements;

- **Cross-OEM interoperability governance:** Ensuring that V2X certificates issued under Indian governance are mutually recognised by all OBU and RSU implementations deployed in India, regardless of manufacturer origin;
- **National vehicular trust infrastructure:** Anchoring India's V2X trust chain within the broader national digital trust ecosystem, enabling future alignment with government digital identity initiatives and cross-sector PKI federation.

This institutional alignment would also facilitate long-term sovereign trust infrastructure: India's V2X PKI, anchored in a statutory body with an existing mandate over national cryptographic trust, would be better positioned for international bilateral trust federation negotiations than a standalone departmental PKI operation. Ambimat Technologies, with its background in PKI system integration, hardware-backed identity architecture, and secure credential provisioning, is available to support such national trust infrastructure as a system integrator partner.

The regulatory framework should explicitly task the DoT and MeitY to engage the CCA at the earliest stage of V2X PKI design, to ensure that the governance architecture for India's vehicular trust infrastructure is institutionally grounded from inception.

4 Security Framework and PKI (Q7)

4.1 Q7: Security Framework for ITS/C-V2X

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

Response: A dedicated V2X security framework is the single most important technical decision in this consultation. Without it, all other investments are vulnerable.

4.1.1 The Core Security Problem

V2X safety depends on the recipient trusting that a received message genuinely originated from the claimed sender. A V2X PKI is architecturally unlike general- purpose web PKI because:

- It must issue **pseudonymous certificates** allowing message authenticity verification without exposing vehicle identity;
- It must support **high-speed certificate refresh** an OBU may request new pseudonymous certificates every few minutes to prevent tracking;
- It must maintain **revocation infrastructure** capable of near-real- time propagation across a national RSU network;
- It must govern **certificate lifecycle for devices**, not humans provisioning, rotation, and revocation must be automated and hardware- integrated, operating at scale across tens of millions of OBUs.

4.1.2 Recommended PKI Architecture

Entity	Role and Governance
V2X Root CA	National trust anchor. Physically and logically separate from RCAI. Governed under CCA / DoT statutory oversight.
Enrolment Authority (EA)	Verifies that OBU/RSU is a genuine, MTCTE-certified device. Issues long-lived Enrolment Credentials. Hardware-bound identity verified at this stage: key must reside in a certified secure element.
Authorisation Authority (AA)	Issues short-lived Pseudonymous Certificates to enrolled OBUs for message signing. AA does not need to know vehicle identity only verifies a valid Enrolment Credential.
Certificate Revocation	CRL distribution via RSU broadcast for offline OBUs; OCSP-like infrastructure for connected endpoints; emergency revocation path for compromised RSUs.

4.1.3 Governance Recommendation

- **CCA (MeitY)** as statutory oversight body for the V2X Root CA;
- **A dedicated V2X PKI Operating Entity** (DoT/C-DOT or authorised PSU) for day-to-day EA/AA operations;
- **TEC** defining PKI requirements, certificate profiles, and testing standards;
- **CERT-In** for security incident response and PKI compromise reporting.

4.1.4 Coexistence with RCAI / X.509 Legacy PKI

V2X PKI uses IEEE 1609.2 certificate formats, distinct from X.509 but interoperable at the cryptographic primitive level (both use ECDSA-P256). We recommend:

1. V2X PKI operates as a *parallel hierarchy*, not a sub-CA of RCAI;
2. Cross-recognition for non-safety V2X contexts is deferred until the primary safety framework is operational;
3. X.509-based PKI remains appropriate for RSU-to-platform backhaul (TLS).

4.1.5 Hardware Requirement for V2X Key Security

V2X identity keys (Enrolment Credentials and Pseudonymous Certificate private keys) **must be stored in a hardware-isolated secure element** within the OBU or RSU. Software-only key storage is insufficient because:

- OBUs are deployed in vehicles a stolen or damaged OBU must not leak its identity credentials;
- RSUs are deployed at roadsides a compromised RSU could sign false messages using a valid certificate;
- ETSI TS 103 097 and IEEE 1609.2 both assume tamper-resistant key storage.

The secure element architecture for V2X deployments must support the following functions as verified, hardware-enforced capabilities:

- **Secure key generation:** Cryptographic key material for both enrolment credentials and pseudonymous certificates must be generated within the tamper-resistant boundary, using certified random number generation.
- **Secure key injection:** Where keys are provisioned externally (e.g., at manufacturing time), injection must occur under cryptographic wrapping (SCP03 or equivalent), such that plaintext key material is never present outside the secure element.
- **On-demand key rotation and update:** The architecture must support operational key rotation over the air without requiring device recall, while the root enrolment credential remains immutably bound to the hardware.
- **Secure signing and verification:** ECDSA-P256 or P-384 signing of V2X messages, and verification of received V2X message signatures against PKI trust anchors, must execute within the secure element.
- **Hardware-isolated cryptographic execution:** All cryptographic operations must execute within the hardware boundary, with the host MCU accessing only the operation result never the key material.
- **Certificate lifecycle management:** The secure element must maintain enrolment credential integrity, support receipt and storage of pseudonymous certificate batches, and enforce certificate expiry and rotation schedules as directed by the AA.
- **Tamper resistance and anti-cloning:** Active tamper detection, voltage and clock fault countermeasures, and hardware uniqueness enforcement must prevent device cloning and physical key extraction.
- **Attestation:** The secure element must produce hardware-signed attestation responses enabling the Enrolment Authority to verify that key material resides in a certified secure element, not in software.
- **Secure provisioning:** Manufacturing-time credential injection must occur on a controlled, audited provisioning line under HSM-backed key custody.
- **Secure firmware trust validation:** The secure element must gate OBU/RSU boot on cryptographic verification of the firmware image, preventing execution of unauthorised or tampered firmware.

The architecture must additionally be designed for future scalability to support: national V2X PKI expansion to tens of millions of enrolled OBUs; high-frequency pseudonymous certificate rotation (potentially every few minutes per OBU); over-the-air credential updates and revocation propagation; trust revocation without device recall; and long-term sovereign vehicular trust ecosystems as India's ITS infrastructure matures.

Architectures similar to secure embedded trust modules such as the AmbiSEC platform demonstrate how hardware-backed PKI identity, secure signing, lifecycle credential management, and cryptographic trust enforcement may be integrated into ITS ecosystems. Such platforms provide an indication of the technical direction that India's V2X hardware specification process should reference when defining the minimum secure element capability baseline for MTCTE compliance.

MTCTE testing requirements (Q5) should explicitly mandate hardware-backed key storage and the full set of cryptographic lifecycle functions described above as pass/fail criteria, referencing TEC 31318:2021 secure element specifications and the ETSI TS 102 941 V2X trust management framework.

5 Spectrum Framework (Q8–Q11)

5.1 Q8: Spectrum Assignment Framework

(a) Partitioning for safety vs. non-safety: Yes. The 30 MHz allocation (5,875–5,905 MHz) should be partitioned:

- Channels 172–178: Safety-critical applications (BSM/CAM, DENM, emergency notification) lowest latency, highest priority;
- Channels 180–184: Operational/non-safety applications (map updates, traffic management, tolling).

(b) Shared vs. exclusive spectrum: Shared spectrum is strongly preferred for V2X safety communications: 30 MHz is insufficient for exclusive assignment to multiple entities in dense urban environments, and vehicle safety messages must reach all RSUs regardless of which authorised entity deployed them.

(c) Interference management: Adoption of Task Force recommendations for EIRP limits, OOBE limits, RSU antenna height constraints, and minimum protection distance between co-channel RSUs is supported.

(e) Deployment registration: A lightweight notification mechanism (rather than full SACFA clearance) is recommended for RSU deployments. A registration requirement reporting RSU location, antenna parameters, and operator identity to DoT is necessary for interference management and security audit.

(h) Roll-out obligations: Modest obligations for deployment on primary highway corridors (NH network) within 3 years of authorisation.

(i) Spectrum surrender: Voluntary surrender with a 12-month notice period. Involuntary reclamation reserved for sustained non-compliance.

5.2 Q9: Application Processing Timelines

A processing timeline of 30 working days for complete applications is recommended. A pre-application consultation mechanism would reduce incomplete submissions and processing delays.

5.3 Q10: Other Spectrum Suggestions

The framework should anticipate evolution from dedicated 5.9 GHz C-V2X to complementary use of licensed cellular spectrum for V2X Uu-mode communications as NR-V2X matures.

5.4 Q11: Security Lifecycle Framework

The regulatory framework must address the full security lifecycle:

1. **Manufacturing:** PKI enrolment credentials must be provisioned at manufacturing time, in a controlled environment, by operators authorised by the V2X EA;
2. **Deployment:** Certificate lifecycle management (refresh, renewal, revocation) must be automated and function reliably with intermittent connectivity;
3. **Decommissioning:** When an OBU or RSU is decommissioned, its credentials must be formally revoked and its secure element wiped.

6 Financial Framework (Q12–Q26)

6.1 Q12: Spectrum Charges

Should spectrum charges be levied on V2I communication service entities?

Response: Spectrum charges for safety-critical V2X services should be waived or set at a nominal administrative level.

V2X safety applications (collision warning, emergency alerts, pedestrian detection) are public welfare services generating no direct consumer revenue. A fee structure tied to commercial revenue would be meaningless for entities whose V2X services are offered free-of-charge as safety infrastructure.

Recommendation:

- Safety-channel spectrum: No spectrum charges, or a nominal administrative fee covering regulatory oversight costs only;
- Non-safety channel spectrum: A modest flat fee commensurate with actual commercial activity.

6.2 Q13–Q16: Spectrum Charging Methodology

AGR-linked charges are inappropriate for entities whose primary function is safety infrastructure, not commercial service provision. A flat annual fee per RSU site, indexed to CPI, is recommended. This recovers oversight costs without creating a disincentive to deploy.

If charges are levied on non-safety spectrum, a new dedicated V2X service classification should be created in the DoT framework rather than analogising to existing radiocommunication service categories.

6.3 Q17: Revenue Sources

Potential revenue sources include: tolling and parking data services; road condition and environmental data services; V2X-enabled fleet management; OEM data integration services; and government contracts with highway authorities and municipal bodies. Safety-critical V2X services should remain unmonetised infrastructure.

6.4 Q18–Q20: Revenue Definitions

For V2I authorised entities:

- **GR:** All revenues from V2X-related commercial services;
- **ApGR:** GR minus revenues from safety-critical V2X message services;
- **AGR:** ApGR minus interconnection charges, roaming charges, GST, and revenues attributable to non-V2X activities.

Safety-related V2X services should be excluded from AGR. The definition of "safety-related" should be tied to the specific message types and channels designated under the spectrum partitioning framework, not left to subjective determination.

6.5 Q21–Q26: Financial Conditions

Condition	Recommendation
Entry fee (Q21)	Rs.5–10 lakhs, covering application processing costs. Not a market-entry barrier.
Bank guarantee (Q22)	Rs.50 lakhs – Rs.1 crore adjusted to deployment scale; linked to roll-out obligations and security compliance.
Net worth (Q23)	Minimum Rs.1 crore for applicants, scaling with geographic scope.
Application fee (Q24)	Rs.10,000–25,000; cost recovery only.
Authorisation fee (Q25)	Safety spectrum: nil or nominal. Non-safety commercial spectrum: 1–2% of AGR.
Additional conditions (Q26)	Annual compliance reporting; security audit certification; financial penalty for security non-compliance; provisions for asset transfer or spectrum return on market exit.

This document constitutes the formal stakeholder submission of Ambimat Technologies Pvt Ltd to TRAI's Consultation Paper on Regulatory Framework for V2X Communication (CP No. 30/04/2026).