सड़क परिवहन
एवं राजमार्ग मंत्रालय
MINISTRY OF
ROAD TRANSPORT
AND HIGHWAYS

सत्यमेव जयते

International Workshop on the Global Navigation Satellite System (GNSS) based Electronic Toll Collection in India

Toll Charger Panel

Panelists for Toll Charger Sessions

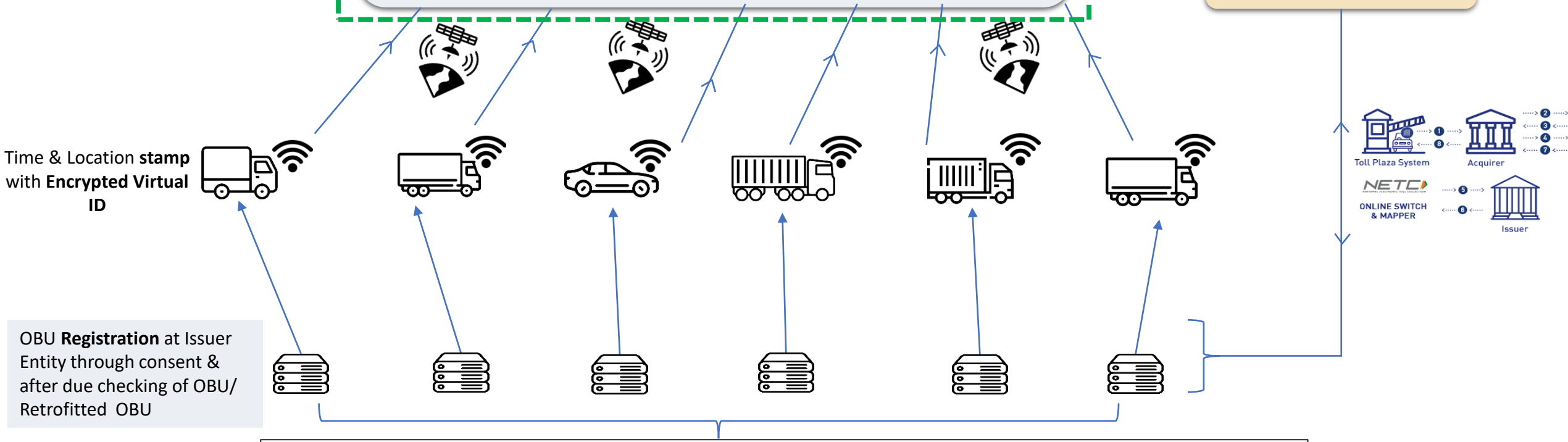
1. Prof Manindra Agrawal, Director, IIT-Kanpur
2. Prof Subrat Kar, IIT Delhi
3. Mr Roopesh Jenu, Scientist-E, C-DAC
4. Mr Wim Vanbelle, CTO, BE Mobile (Belgium)
5. Mr Peter Kozej, Sky Toll (Slovakia)
6. Mr , Senkathir “Selvan” Suriaprakasam, IoT Division, TCS
7. Mr Jasvinder Grewal, Principle Architect, Public Sector, Google India
8. Mr Norbert Schindler, CEO, GNSS Consulting (Austria)
9. Mr Pavan Teja, CEO, AutoSure AI, India

Toll Charger Engine

1. **Map Matching by pings from OBU**
2. **Distance Calculation**
3. **Toll Calculation against Virtual ID, Toll Parameter and Vehicle Class**

Toll Charge

Payment System similar to existing FASTag



OBU **Registration** at Issuer Entity through consent & after due checking of OBU/ Retrofitted OBU

The system **will** follow 01 Vehicle - 01 OBU Policy. For any change in OBU Issuer, the Vehicle Owner has to first decouple with existing Issuer Entity.

Role of Toll Charger

- High Level Role of Toll Charger
  - Map Making of GNSS stretch
  - Receive anonymized data from OBUs
  - Map Matching
  - Calculation of Distance Travelled
  - User Fee Calculation
  - Send User Fee to Acquirer Bank
  - User Fee Portal for each Toll Plaza
  - Grievance Redressal through Issuer Entity
  - Integration with GNSS Lanes and Fraud Detection
  - OBU onboarding and registration protocols
  - Other applicable roles and responsibilities

Key Requirements/Non-negotiables

- Toll revenue should be protected.
- Data should come directly from the Vehicle to Toll Charger or Gateway in ownership of NHAI.
- Strict Adherence to SLAs/Uptime of Toll Charger Core
- Architecture designed for toll-charger interoperability
- Cloud/Data Center should be as per MEITY policy
- End to End encryption of data
- Ownership of TC software and maps will remain with NHAI

Map-Making 🗺️

Map-making will be the responsibility of the Toll-Charger
Ownership of the map will lie with NHAI

Discussion

- If TC builds map from scratch:
  - Existing Open Source Maps can be basis to start with map-making
  - It should add additional meta-data useful for overall NHAI ops
- If TC commercially sources the map:
  - Perpetual license or such agreements will be preferred.
  - API access of map if provided should be vector based.
  - Experience internationally has been that local map providers keep data more updated
- In both cases, map standards need to be pre-defined (format, attributes, accuracy etc) to ensure TC interoperability.

Map-Matching

TC should be able to apply digital routing/Gap analysis tools to validate derouting / fraud / loss of signal / OBU malfunction cases.

Discussion

- But not all algorithms are AI based; map-matching should be only functionally defined.
- Collecting location data every minimum 5 seconds is good enough without overworking the GNSS sensor or causing excessive noise, data usage, or storage issues.
- Flyover vs service roads: Altitude data is a must, maps should also have z values.

Data Governance/Security 🔐

There should be no revenue loss. Toll Charger should take care of security.

Risks	Mitigation
Spoofing: Data sent to TC appears to come from OBU but is actually generated from a computer program.	Digital Certificates, Public-Private Key or Hardware Security Module to be used. TC will have Key Management Module. TC to have algorithms to detect simulated data in conjunction with Enforcement Gantries
Man-in-the-Middle Attack: Data from the On-Board Unit (OBU) is intercepted and altered before it reaches the Toll-Charger.	End to End encryption from OBU to TC
Identity Theft: Data from Passenger A's OBU is manipulated at the source to make it look like it belongs to Passenger B.	Employ unique, secure identifiers for each OBU only known to User/Issuer Entity.

Data Governance/Security 🔐

There should be no revenue loss. Toll Charger should take care of security.

Risks	Mitigation
Firmware Tampering: User boot loads or modifies firmware provided by OBU manufacturer after registration to TC	Firmware integrity checks through key provided by OBU manufacturer.
Physical Tampering: User unplugs/switches off OBU after passing toll-plaza	Tamper-resistant casing; can inform to TC/IE if tampered. OBU can have battery to collect and send data for few hours even if disconnected.
Data Leakage: Leak at Toll-Charger can lead to risking of commercial traffic etc.	Storing encrypted data at Toll Charger; High security checks; Limited data collection; deletion after purpose achieved
Single Point of Risk when TC Server Down/Disaster, Distributed Denial of Service attacks.	Disaster recovery – active redundancies and fail-over mechanisms; Gateway/TC URLs should be secret.

Data Governance/Security 🔐

- Quality Checks occur at three stages:
  - Accreditation at the manufacturing level
  - Quality check before onboarding OBU by IE including installing certificates/private keys
  - Continuous quality checks by TC/IE on streaming data

These discussions are crucial for system architecture and OBU specifications and should be finalized before proceeding.

Scale and Architecture

Data from OBU should come to TC directly; System Architecture should allow scale, interoperability and security

__ million commercial vehicles in India; ___ ply a highway on a given day; data/server/bandwidth costs will depend on:

Scale Factors	Solutions
Data Collection Frequency	Location-time data at every 5 seconds is good for map-matching.
Data Sending Frequency	Data can be collected at above frequency but OBU can send consolidated packet at 60 second frequency to reduce server interaction
Data Packet Size	The data packet (keywords etc) should be minimal to reduce data costs
Number of Commercial Vehicles Overall V/S Subset on NH at a given time	Layered architecture with gateways that can filter non-highway data before core Toll Charger processes data

Scale and Architecture

- Layered Architecture: Government administered/owned Gateways are necessary between Toll-Charger Core and Vehicle data for scale, interoperability etc to act as proxy.
- Gateways can be geography wise etc.
- Toll Charger will maintain Vehicle Onboarding Portal wherein Issuer Entity will be given access to register GNSS consumers/OBUs in standard manner. This will have integration with VAHAN Database.
- Above module will also manage key authentication with OBUs, end to end encryption etc.
- The data interchange formats between OBU, Issuer Entity, Toll Charger and Gateway should be standardized (UPI approach)
- Architecture should be such that if Issuer Entity or OBU provider shuts down, it is easy for consumer to transition to other Issuer Entity/OBU.

Integration of GNSS Lanes with Toll Charger

Integration with GNSS Lane: The Toll Charger shall integrate with the GNSS Lanes of the Toll Plaza

- There must be real-time interaction between enforcement gantries/Toll plazas and GNSS Toll Charger for a good enforcement support system.
- There can be Enforcement Gantries (apart from Toll Plaza) at strategic locations on highway to avoid revenue loss. Mobile APNR units can also be used.
- Enforcement Gantries can follow NHAI's ATMS 2023 VIDES specs with slight modification. This will serve dual-purpose of GNSS and Traffic Violation enforcement.
- The ownership and operation of the Enforcement equipment would be from a different entity than the TC (e.g. the concessionaire, SIs).

Red/Green OBU

Toll-Charger will be hold single source of truth on RED/GREEN OBUs | Red OBUs will need to pay 2x Toll in GNSS Lane

- Need to clearly define situations wherein an OBU is considered RED.
- OBU may be RED for reason out of consumer's control. They need to know real-time status before entering GNSS Lane.
- User can know status through SMS or Rajmargyatra app.
- There should be a single entity in-charge of the red/green status (toll-charger) but it can aggregate data from other stakeholders
- Any APIs for red/green have to be real-time in practice unlike blacklist status at present.

Grievance Redressal System ⏱️

Issuer Entity will provide grievance redressal system as provided in FASTag.
Toll Charger will provide data, map etc to Issuer Entity for this purpose.

- Single Online Dispute Redressal (ODR) portal will be created by Toll Charger which will provide data to Issuer Entity.
- Consumer will submit complaint to Issuer Entity
- ODR module will have data from OBUs, Enforcement Gantries, Toll Plaza etc. to effectively close the complaint.
- This portal will have integration with 1033/Rajmargyatra app as well.

Value Added Services – Government 🚨

- The overall objective should be to help reduce logistic costs in India using an eco-system approach
- Same OBU/Data shall have usecases > number of ports on OBU.
- We follow standardized user-consent based data-sharing for Value Added Services similar to RBI's Account Aggregator Framework or Ayushman Bharat Digital Mission.
- Government User Cases: We may identify over-speeding, contraflow on highways and other traffic violations.
- Architecture can be used for congestion pricing etc in the future.


Thank You
Project – Bengaluru Mysuru Access Controlled Highway

Accelerating qualitative GNSS rollout | Wim Vanbelle, CTO, BE-Mobile

- Automate accreditation to the highest degree possible
  - To cover the time constraint risk on the VLT/OBU devices, automation for accreditation is highly recommended to the highest degree possible.
    - Initial accreditation tests for new hardware, continuous KPI monitoring for active fleets

- Use of a middle-tier OBU Proxy can cover advanced features, so the OBU does not have to.
  - Avoids rollout of separate OBU Proxies for different OBU/VLT devices
  - Centralize security measures
  - Support for privacy feature in the middle-tier before the feature is present in the OBU firmware.
  - Exchange of geozone/filter areas with OBU/VLT's (and support for dynamic GNSS frequency zones)
  - Allow for easier support for multiple map-matching toll domains

- Apply smart and focused enforcement
  - Smart barrier management for the GNSS lanes (period closure of GNSS lanes)
  - Strategically positioned gantries/mobile enforcement units result in future proof networks
  - Efficient use of enforcement resources through backend smart fraud detection and ranking features, in support of OBU/VLT security measures