Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

Connected Mobility Ecosystem - V2X in Digital Trust PKI

PUBLIC KEY INFRASTRUCTURE BASED DIGITAL CERTIFICATES FOR CONNECTED VEHICLES (V2X)

Dr. Ir. K K Soundra Pandian
Ph.D (IIT Patna), PDF(NYU)
Scientist ‘E’, Govt. of India
Ministry of Electronics and IT,
O/o CCA, New Delhi

AGENDA

PUBLIC KEY INFRASTRUCTURE BASED DIGITAL CERTIFICATES FOR CONNECTED VEHICLES (V2X)

- Indian Secure Trust: The PKI Landscape
- Introduction to V2X and PKI for V2X
- CCA PKI Framework
- Overview: GLOBAL STANDARDS: IEEE 1609.2 / ETSI 102 940
- ITS Deployment Within PKI Ecosystem

Indian Secure Trust : The PKI Landscape

1. India has a strong trust backbone built based on Public Key Infrastructure (PKI)
2. The PKI in India is governed by the Indian Information Technology Act, 2000, and the Controller of Certifying Authorities (CCA) under MeitY is the regulatory body for PKI in India.
3. PKI/ Trust Services are operated by 20+ Service Providers under the National PKI framework
4. India has one of the largest user bases for e-Signed transactions.
    - 10 million + active long lived certificates enabling billions of transactions every day
    - 400 million+ short lived certificate transactions using eSign initiative under Digital India Programme.
5. India has legal validity for these signatures, with admissibility in the court of law.
6. India conforms to global Public Key Infrastructure practices, putting it on par with other major countries/economics.
7. India has a vast implementation of an e-signature ecosystem, on which the country's Digital

Role of CCA: Evolving Context

- Identify the constraints in the large-scale adoption of electronic signatures and explore the options to promote the same
- Examine the standards used in the existing India PKI system and the need for upgradation in line with the emerging security trends. E.g. SHA2, RSA, ECC, Key Size, storage medium, etc
- ***Examining the feasibility of the adoption of new standards and preparing for a migration plan. For e.g., PQC***
- Examining the emerging areas where digital signatures can be used to secure the device or transaction, e.g., IoT, V2X, Drone, smart city, blockchain, etc
- Indigenization of the components involved in the digital signature ecosystem e.g., Browser development, crypto token, or any other key storage medium.

PUBLIC KEY INFRASTRUCTURE (PKI)



ROOT CERTIFICATE AUTHORITY (RCA)

- The highest level of trust
- Signs intermediate certificates using private key

INTERMEDIATE CA (ICA)

- Acts on behalf of the RCA to reduce load.
- Issues certificates

END ENTITY CERTIFICATE

- Installed at end entity to prove its identity
- Signed by ICA

PKI Enables

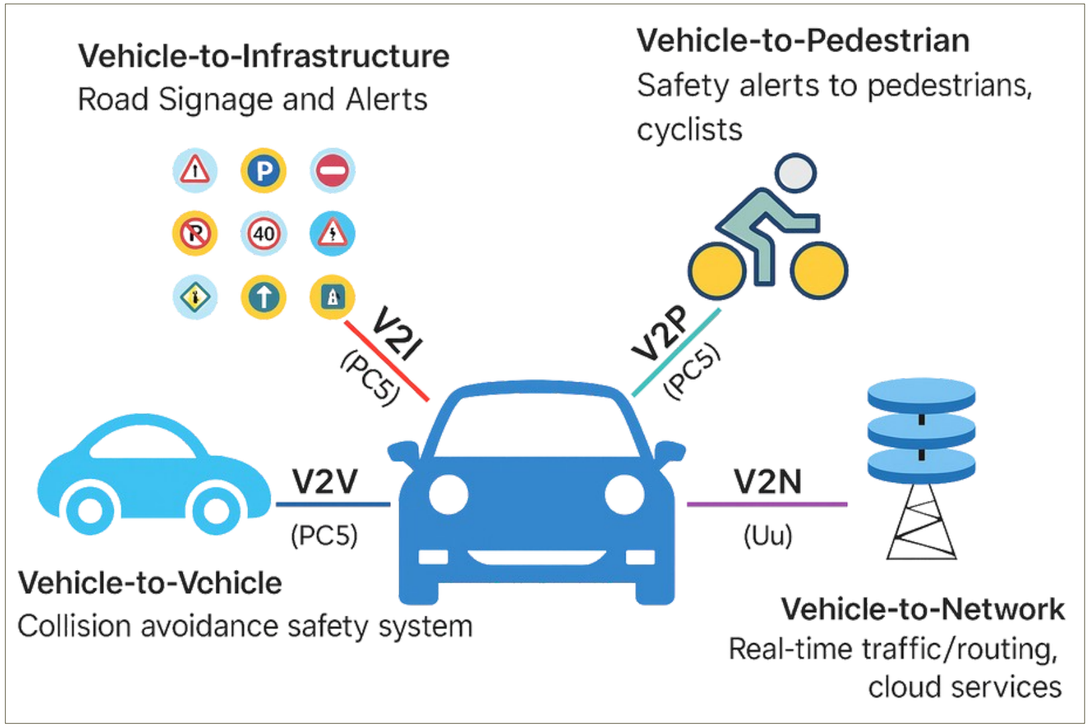
- Trust Anchors (through trusted CAs)
- Authenticity (via Digital Signatures)
- Digital Certificates Provisioning

VEHICULAR COMMUNICATION (V2X)

ABOUT

- Cooperative Communication between Vehicles and
  - **Like-minded Vehicles (V2V),**
  - With Roadside Infrastructure, (V2I or I2V)
  - Vulnerable Road Users - Pedestrians, 2-wheelers, 3-wheelers (V2VRU or V2P)
  - And other elements of the transportation ecosystem, esp Networks (V2N).





V2X SECURITY

AN ESSENTIAL ELEMENT OF SUCCESS IN V2X ARE STRONG SECURITY CONSTRUCTS

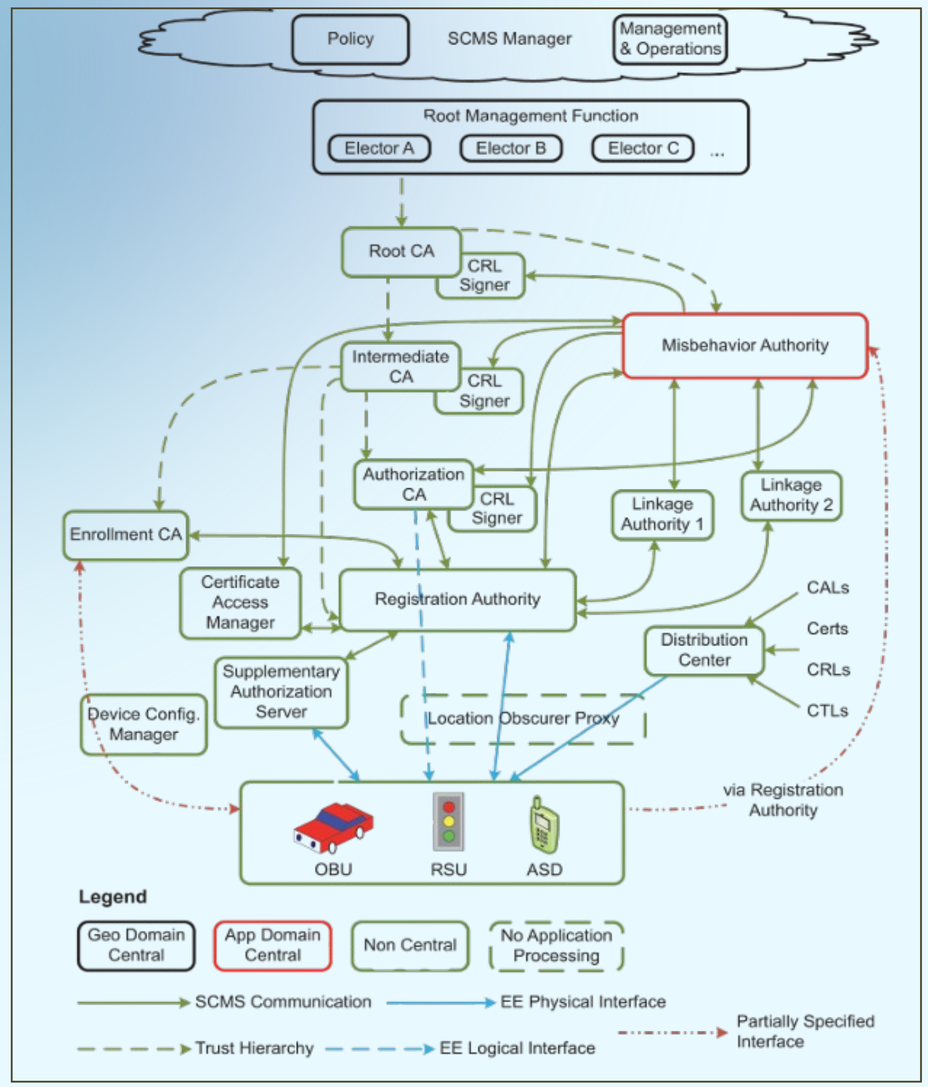
- Ensure **Trust**, **Confidentiality**, **Authenticity** and **Integrity**
- **Protect Privacy** of end users and
- Resilience to Attacks that could compromise safety and public confidence.

GOALS OF SECURITY IN V2X: ENABLE VEHICLES AND INFRASTRUCTURE TO

- Trust the Authenticity of transmitted data,
- Make Accurate Decisions, founded on reliable data,
- Protect Privacy

PUBLIC KEY CRYPTOGRAPHY (PKI) BASED DIGITAL CERTIFICATES PROVIDES THE RIGHT SOLUTION FOR SECURE CREDENTIAL MANAGEMENT IN V2X

GLOBAL STANDARDS: IEEE 1609.2



SECURITY CREDENTIAL MANAGEMENT SYSTEM (SCMS)

- PKI Architecture specified in IEEE 1609.2.1
- Provision End Entities with Digital Certificates
- Certificates Ensure Trust, Authenticity, Integrity, Confidentiality, and Pseudonymity

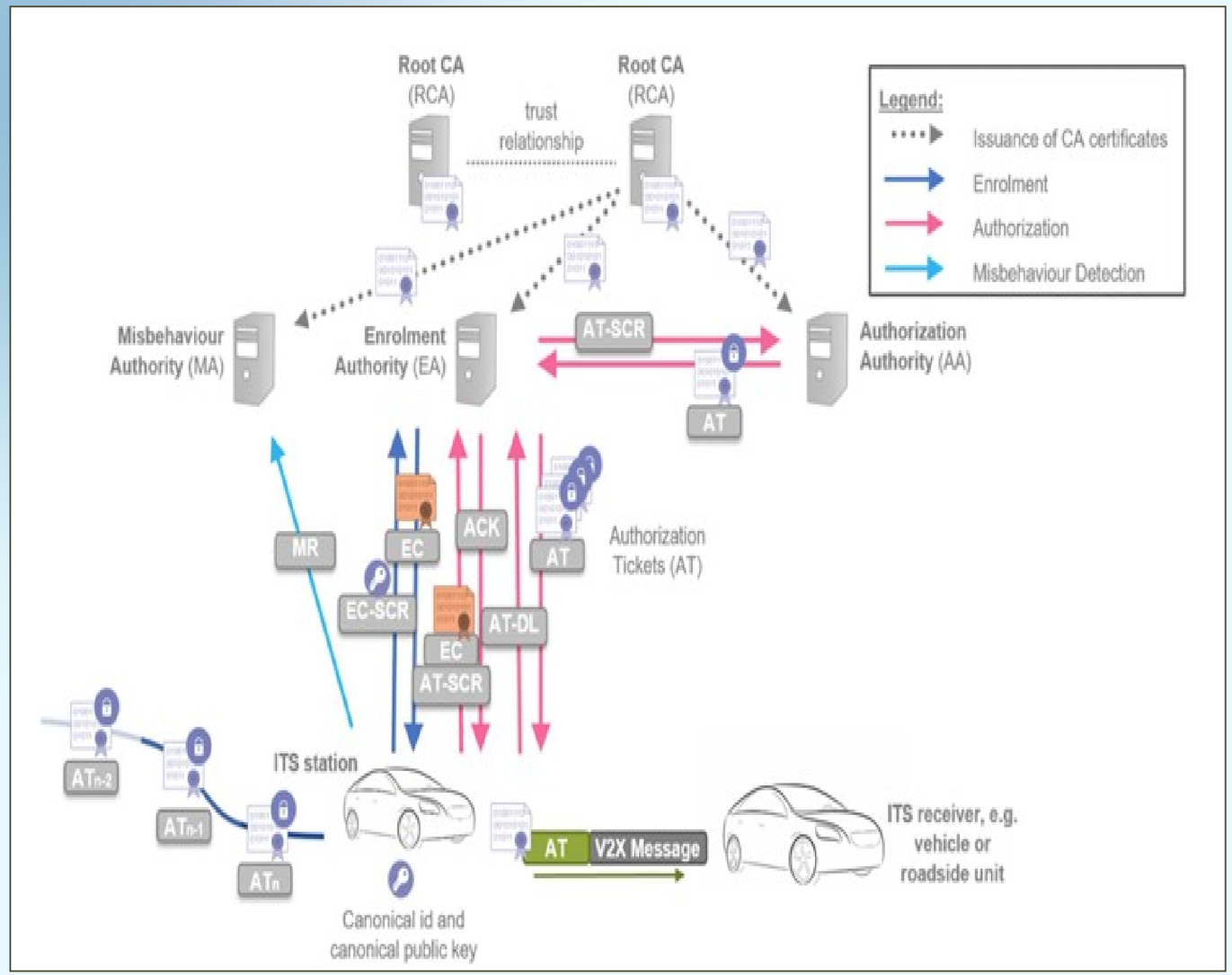
TRUST MODEL SPECIFIES AN I.T.S ROOT CA HIERARCHY

- SCMS Manager Designates the ROOT CA
- Intermediate CA is authorized by the RCA
- ICA authorizes subordinate CAs - ECA, ACA and MA
- Subordinate CAs issue and manage EE certificates

ROLES OF SUBORDINATE CAS

- ECA issues a Long-Term Identifier to the EE
- ACA issues application permissions to the EE
- Registration Authority (RA) becomes a CA SPOC for the SCMS
- MA recommends revocation of EEs to CRL Signers and RA

GLOBAL STANDARDS: ETSI 102 940



COOPERATIVE-ITS SECURITY CERTIFICATE MANAGEMENT SYSTEM (CCMS)

- ETSI 102 940 proposes the PKI Architecture
- Manage Trust and Privacy of ITS-S (ITS Stations).

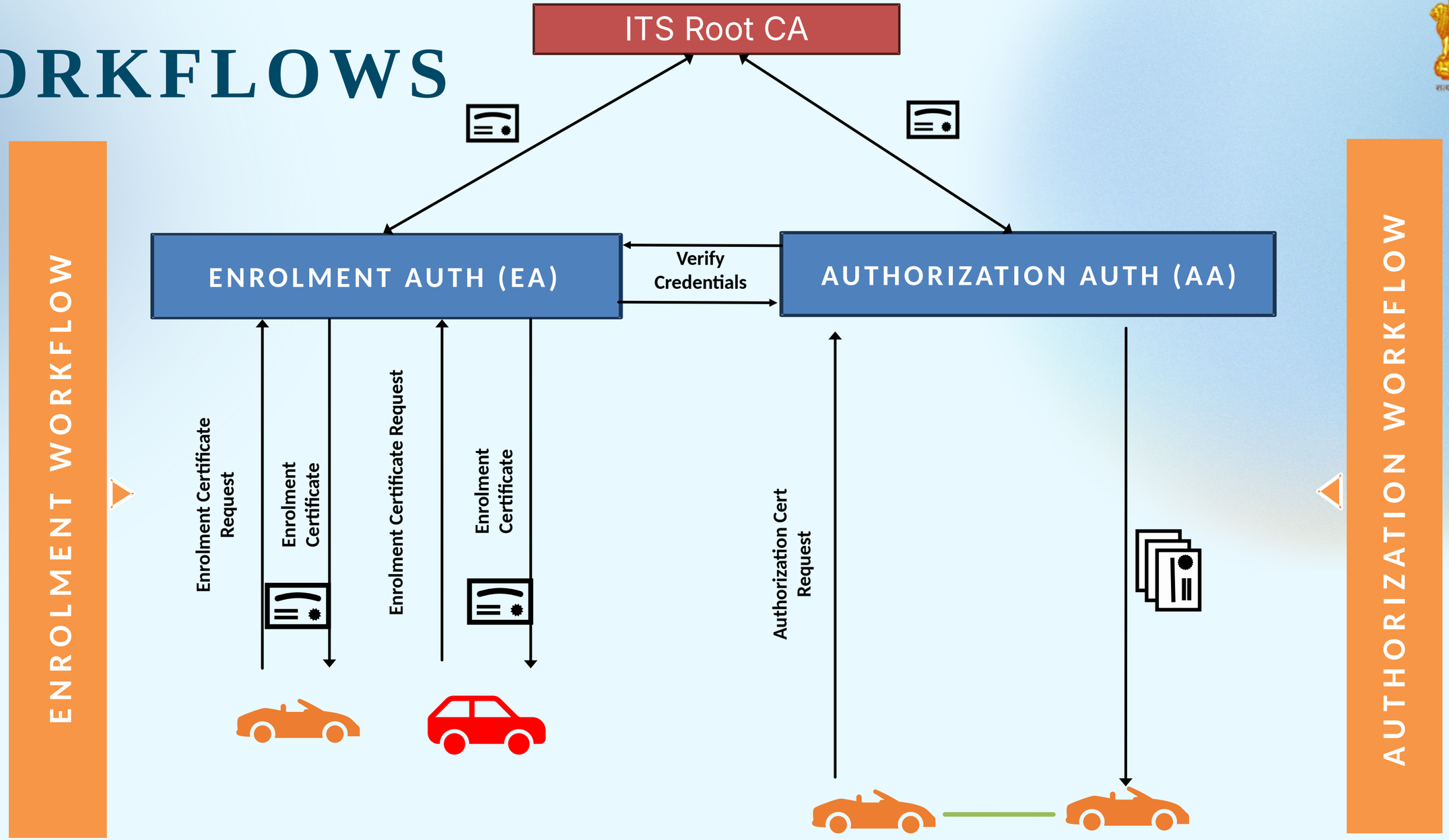
HIERARCHY INCLUDES ROOT CA

- Issues certificates to subordinate CAs, EA, AA, and MA

FUNCTIONS

- EA issues the Long-Term Identity Certificate
- AA issues the Application Permissions
- MA manages the Certificate Revocation List for ITS-S

WORKFLOWS


ITS Root CA
ENROLMENT AUTH (EA)
Verify Credentials
AUTHORIZATION AUTH (AA)
ENROLMENT WORKFLOW
AUTHORIZATION WORKFLOW
Enrolment Certificate Request
Enrolment Certificate
Enrolment Certificate Request
Enrolment Certificate
Authorization Cert Request

INTELLIGENT TRANSPORT SYSTEM DEPLOYMENT WITHIN INDIA'S PKI

STATUS QUO

- The Controller of Certifying Authorities (CCA), under the IT Act, regulates all Certifying Authorities in India.
- Root CA of India (RCAI), managed by CCA, acts as the National Trust Anchor
- Issues X.509-based certificates for Digital Signatures.

CHALLENGES:

- CCA specifies X.509 certificates, whereas V2X communication globally specifies ITS certificates
- Both Certificates are incompatible.

CONSIDERATIONS

- Global Interoperability – Standards Alignment
- Ease of Implementation – Easy to amend; avoid special regulations through policy/law
- National Sovereignty - Ensure Bharat-specific fitments and use cases

THANK YOU!