Development of National Trust Centre for IoT/M2M devices

Shikha Srivastava

Centre for Development of Telematics

Mandi Road, Mehrauli, New Delhi - 110030

Background

Telecom Regulatory Authority of India (TRAI), in its **M2M recommendations** on 'Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications' dated the 5th of Sep 2017, has recommended at Section 5.3, inter alia, that:

a) Device manufacturers should be mandated to implement "Security by design" principle in M2M device manufacturing so that end-to-end encryption can be achieved.

b) The government should provide comprehensive guidelines for manufacturing/ importing of M2M devices in India.

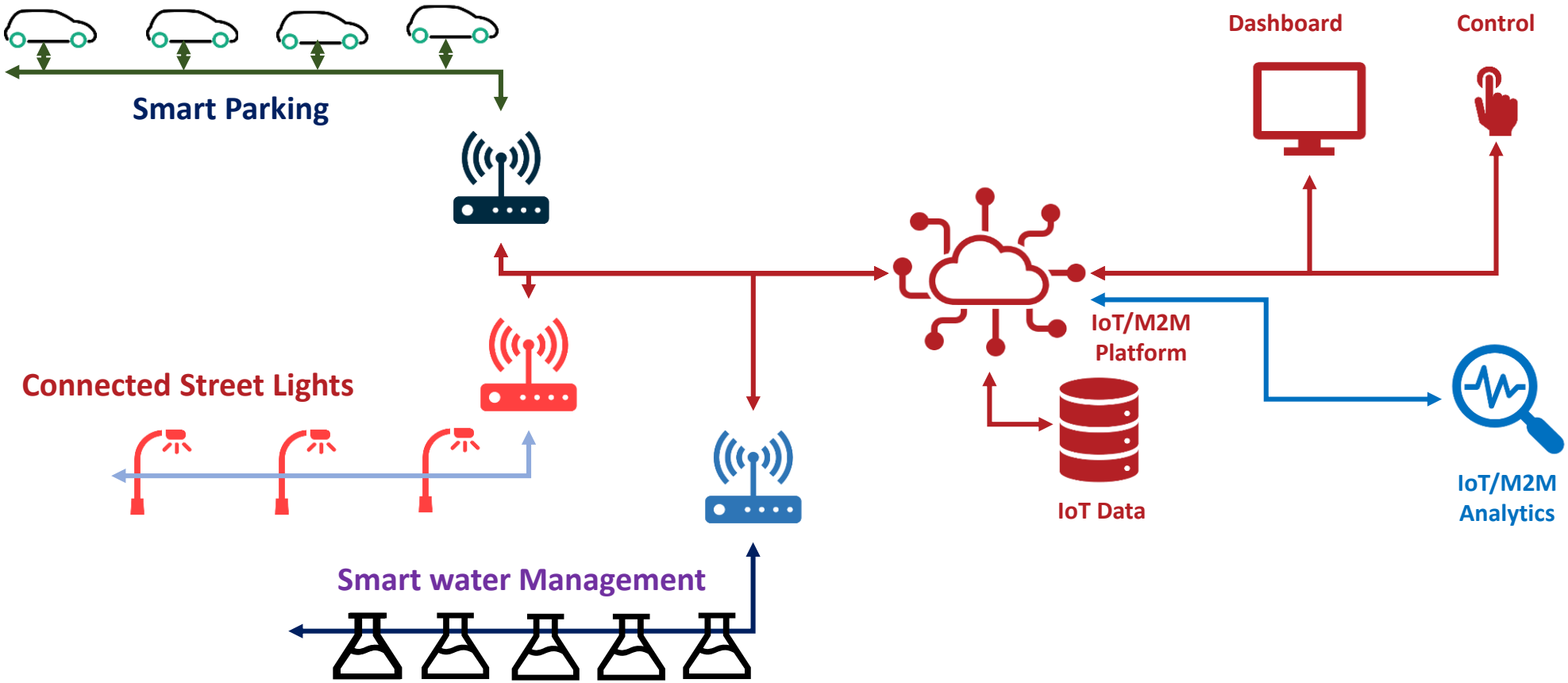
c) **A National Trust Centre (NTC), under the aegis of TEC, should be created for the certification of M2M devices and applications (hardware and software).**

The main requirement is to address the security challenges in the deployment of IoT/M2M Devices and Applications that can pose threats to the custodians and users, its own operation and also potentially harm the networks that it connects to.

Typical IoT/M2M Architecture

- Typical implementations of IoT/M2M solutions follow the architecture shown here.
- The sensing layer contains the sensors and actuators which connect to the gateways using any of the Personal Area Network (PAN) technologies.
- The gateway devices typically connect using any network technologies shown in the Network Layer to the Application Infrastructure Platform shown in the Application Layer.
- The information pertaining to the sensors, actuators, gateways etc. are tightly coupled with the Application Layer entities.

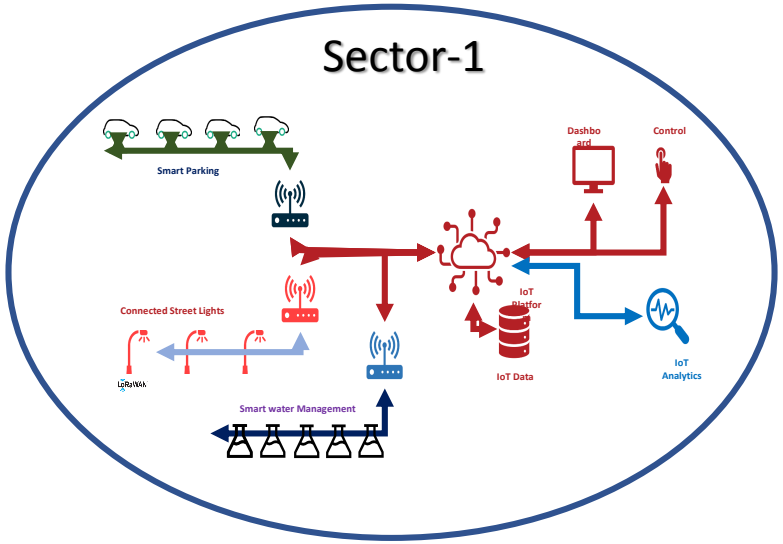
IoT/M2M implementation in Smart Cities

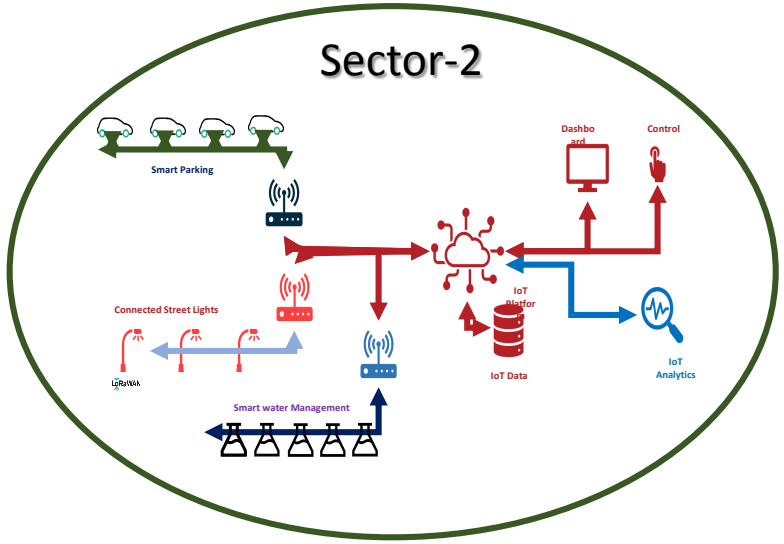


Proprietary, vendor locked-in implementations with proprietary methods of maintaining information about the connected devices and applications.

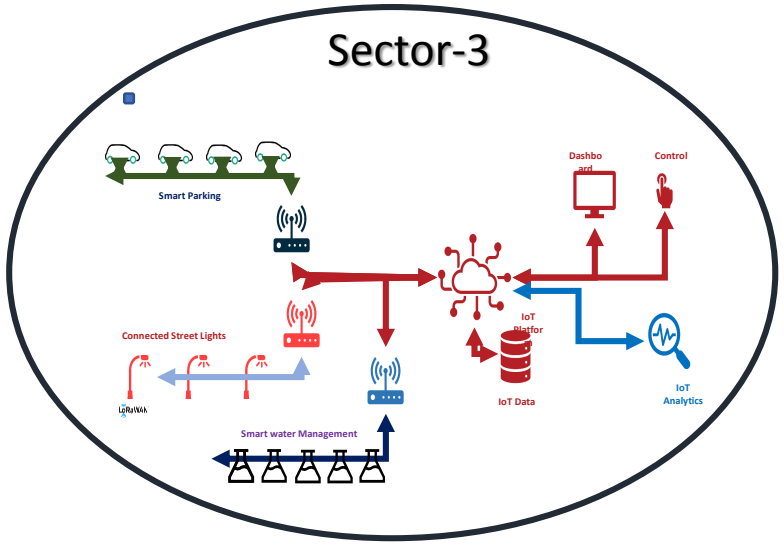
Anonymity doesn't guarantee security

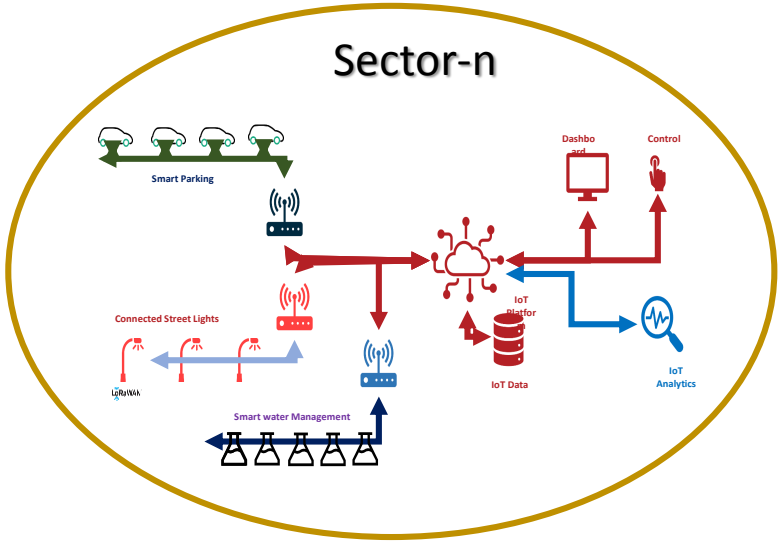
Issues with the proprietary, siloed implementations





- All IoT implementations are isolated and proprietary implementations.
- No centralized mechanism exists to obtain Information regarding connected devices, their manufacturers, their implementers or the domain they are deployed in. Same is the case for the Applications.
- No standard mechanism to establish trust for devices and applications.





Issues contd..

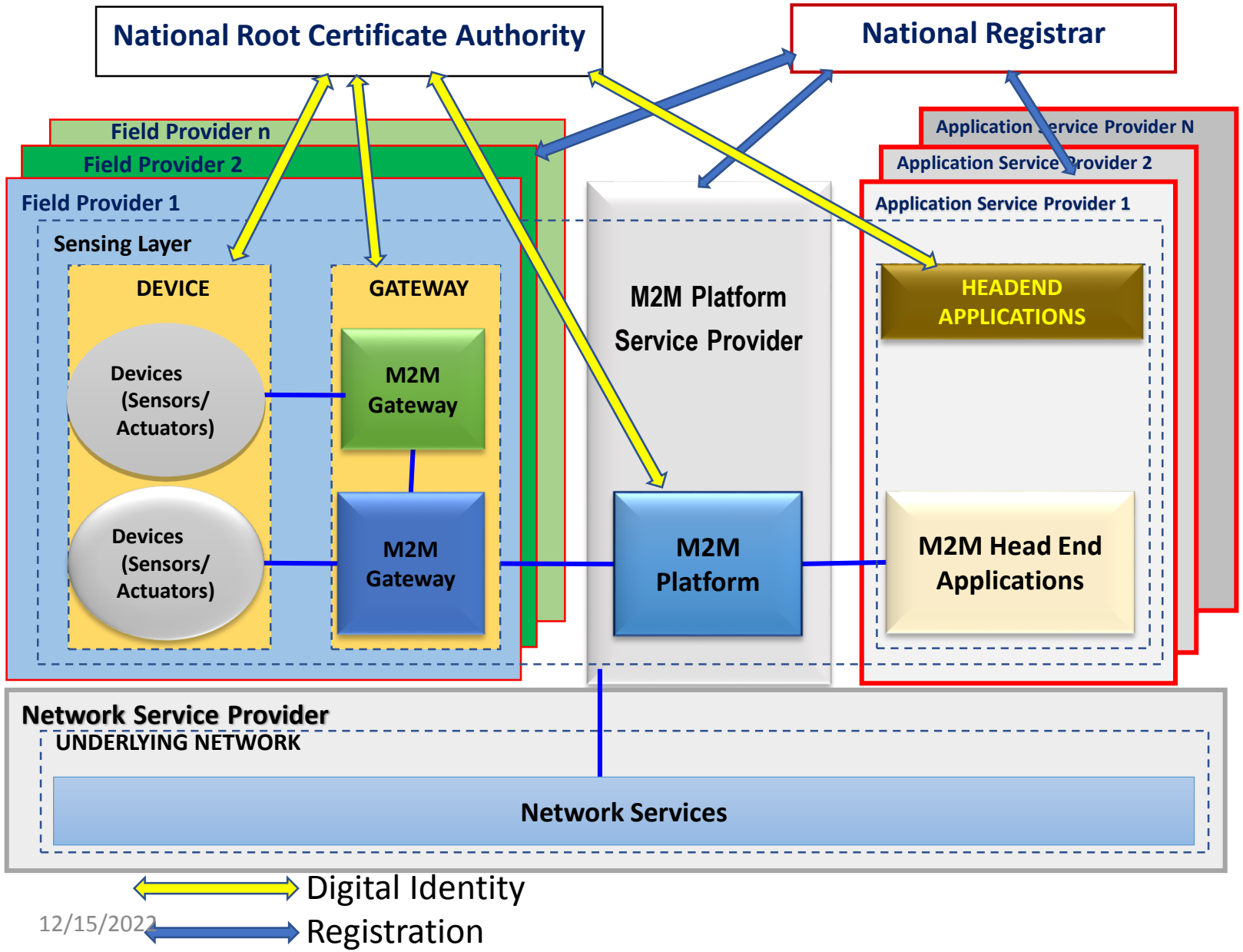
- Any connected device, seemingly anonymous can pose a serious threat to the entire ecosystem e.g. a Smart Traffic Management System which controls the traffic signals in a city, if compromised, can pose a serious threat to life and property

- The vulnerability of any device or application can not be assessed if relevant information pertaining to the device/application is not known.

- Accountability can not be established in cases of security breach in the absence of relevant information about the devices, applications, connectivity, platforms and service providers/stakeholders of the ecosystem.

The foundation of Trust depends on the authentic information about the entity. In IoT/M2M ecosystem, the implementation of security depends on the authentic identity of its entities which include devices, applications, manufacturers, application providers, platform providers and connectivity providers.

Proposed Security Framework for M2M Application Roll Out

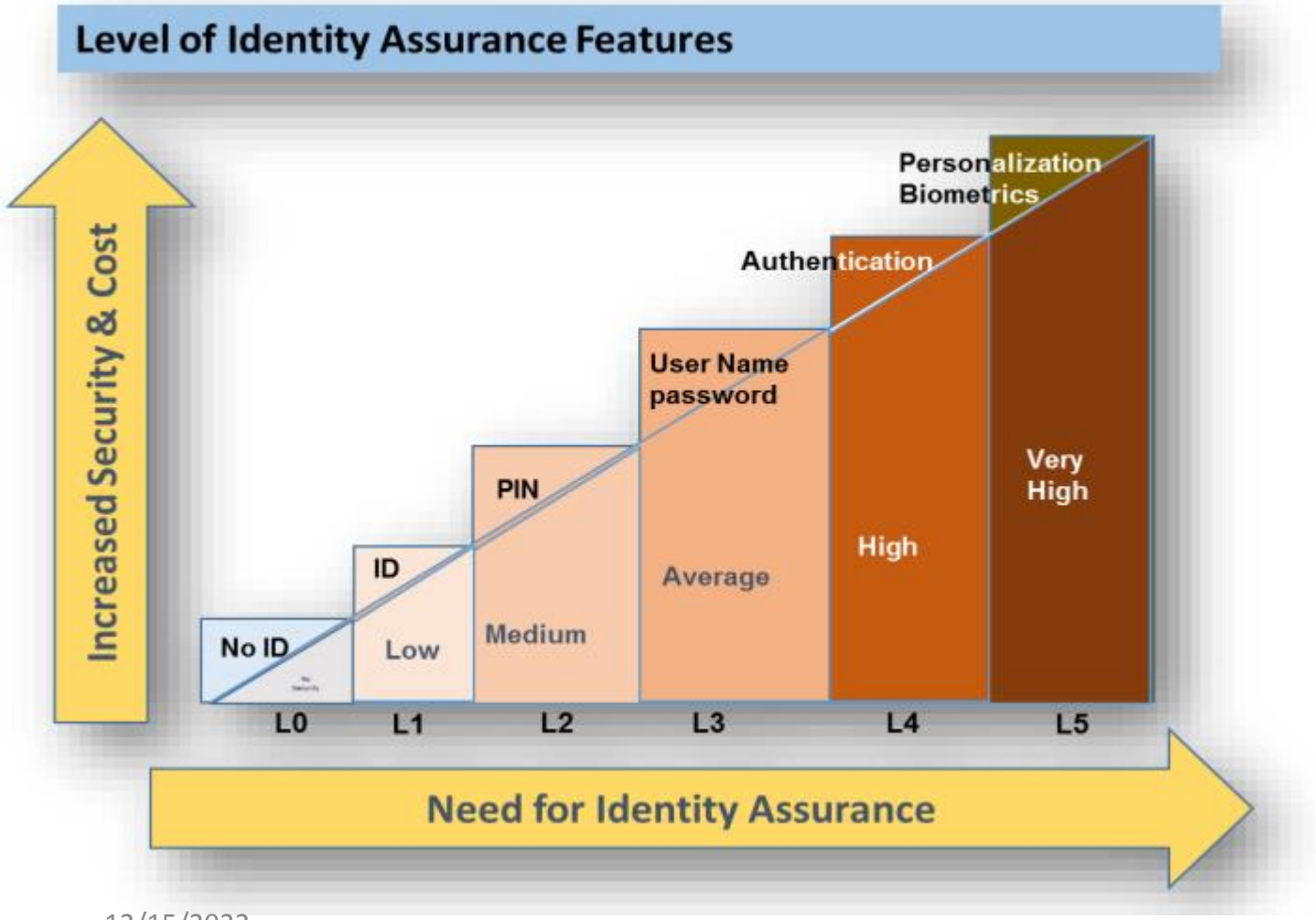


The framework proposed a national registrar taking care of the registration of all entities of IoT/M2M ecosystem e.g. devices, applications, manufacturers, application providers, platform providers and connectivity providers etc.

It also proposed to integrate them all with the National Root Certificate Authority of India

Levels of Assurance for Devices

The diagram below represents the 5 levels of security as defined in the TEC Report on M2M Security. It proposed labeling each device with a level of security so that it becomes easy for the implementers to choose the right device for a specific use case category.



Level 0: No authentication and Identification
Level 1: Identification and Authentication based on defined ID on End Point Device
Level 2: PIN based Authentication and Identification
Level 3: User name and password authentication method
Level 4: By Key exchange and mutual authentication method
Level 5: Biometric authentication

Assurance Levels for End Point Devices

Levels	ID	PIN	User name Password	Authentication PKI infrastructure	Personalize and biometric
L0	X	X	X	X	X
L1	√	X	X	X	X
L2	√	√	X	X	X
L3	√	X	√	X	X
L4	√	X	√	√	X
L5	√	√	√	√	√

The table above recommends certain options for user authentication based on the classification of the Assurance Levels for End Point Devices.

Use Case Class Specific Mandatory Security Requirements

The table below states the mandatory security compliance by Use Case Classification.

Use Case categories	Availability / QoS	Authentication Level	Encryption	KYC	
			Transport Layer	Machine	User
Mission Critical, High QoS, Sensitive Information [CQS]	High	5	Mandatory	Mandatory	Mandatory
Mission Critical, High QoS, Non Sensitive Information [CQN]	High	3		Mandatory	
Mission Critical, Best Effort, Sensitive Information [CBS]	Medium	5	Mandatory	Mandatory	Mandatory
Mission Critical, Best Effort, Non Sensitive Information [CBN]	Medium	2		Mandatory	
Non Critical, High QoS, Sensitive Information [NQS]	High	4	Mandatory	Mandatory	Mandatory
Non Critical, High QoS, Non Sensitive Information [NQN]	High	1		*	
Non Critical, Best Effort, Sensitive Information [NBS]	Low	4	Mandatory	Mandatory	Mandatory
Non Critical, Best Effort, Non Sensitive Information [NBN]	Low	0		*	

The assessment of the Mandatory requirements of Machine KYC for NQN and NBN use case classifications shall be undertaken in consultation with the respective Industry verticals.

Objective of National Trust Centre

To develop a national framework for regulation and establishment of trust in IoT/M2M ecosystem

To design and develop a software platform which will enable a standardized way of information exchange between NTC and all sectorial and siloed IoT/M2M implementations

To create registries of IoT/M2M Devices, Manufacturers, Service Providers, Application Providers and Applications and integrate them all to ensure accountability and Trust in IoT/M2M ecosystem.

To integrate with the Public Key Infrastructure (PKI) framework of Government of India. Thereby bringing all sectorial CAs under the Root Certifying Authority of India (RCAI) established by Controller of Certifying Authorities (CCA)

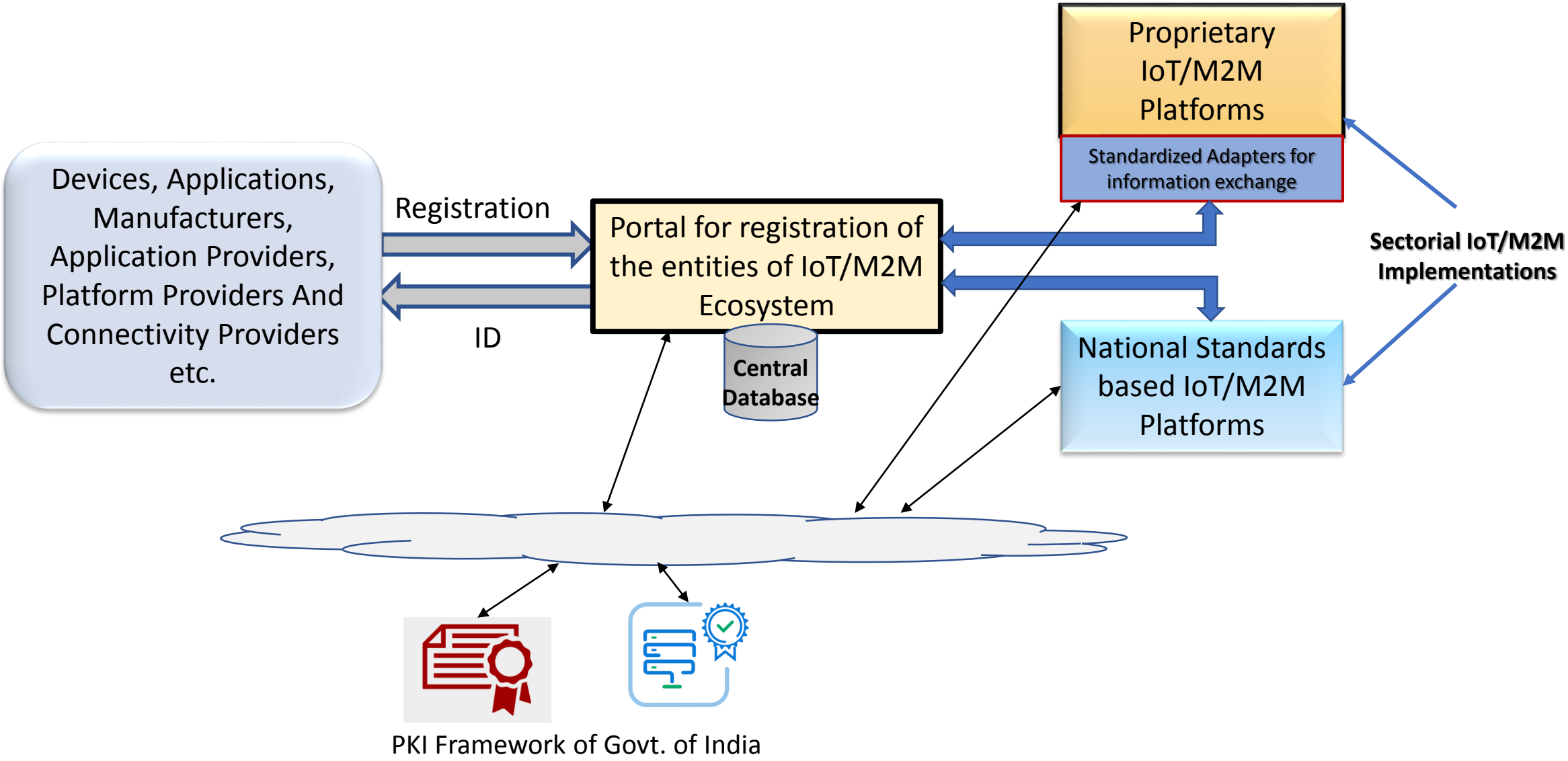
NTC Services

NTC would be offering the following services:

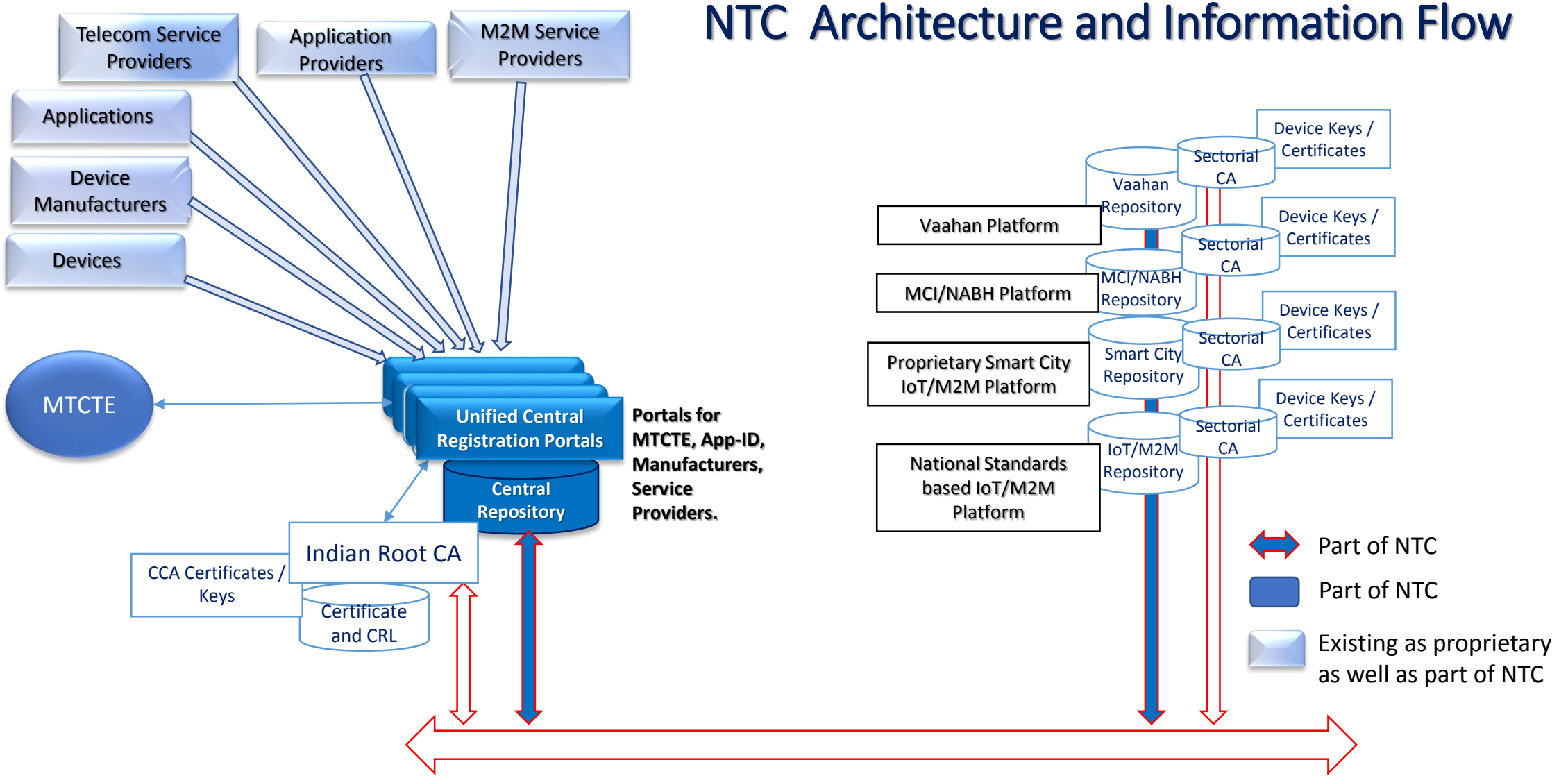
- Registration of M2M/IoT Platform Providers
- Registration of M2M/IoT Application Service Providers
- Registration for Device Manufacturer
- Registration of Certified Connected Devices
- Registration of M2M/IoT Applications
- Registration of tamper resistant end point identifiers

The registration can be done either directly or through the sectorial platforms from where the data would be available to the central registry.

Broad NTC Architecture and Information Flow



NTC Architecture and Information Flow



The registration of devices, applications, platforms as well as their providers etc. would happen both at the central level and well as at the sectorial level. Information pertaining to them would be exchanged mutually between the regional repository as well as the central repository.

Key features of NTC Architecture

- Autonomy to the respective departments/domains/sectors who can continue to implement solutions and maintain their own repositories.
- From a national perspective, it would have a syndication whereby all the autonomous systems would share information under a central authority in a secured, trusted yet user friendly manner.
- Trust establishment by interfacing with the certificate authorities in a hierarchical manner i.e. the sectorial CAs would be part of PKI framework of Govt. of India
- The sectorial IoT/M2M platforms would be able to exchange information with the National Trust Centre using standardized interfaces (to be developed)
- Mandatory Testing and Certification Of Telecommunication Equipment (MTCTE) portal of TEC would be integrated with NTC

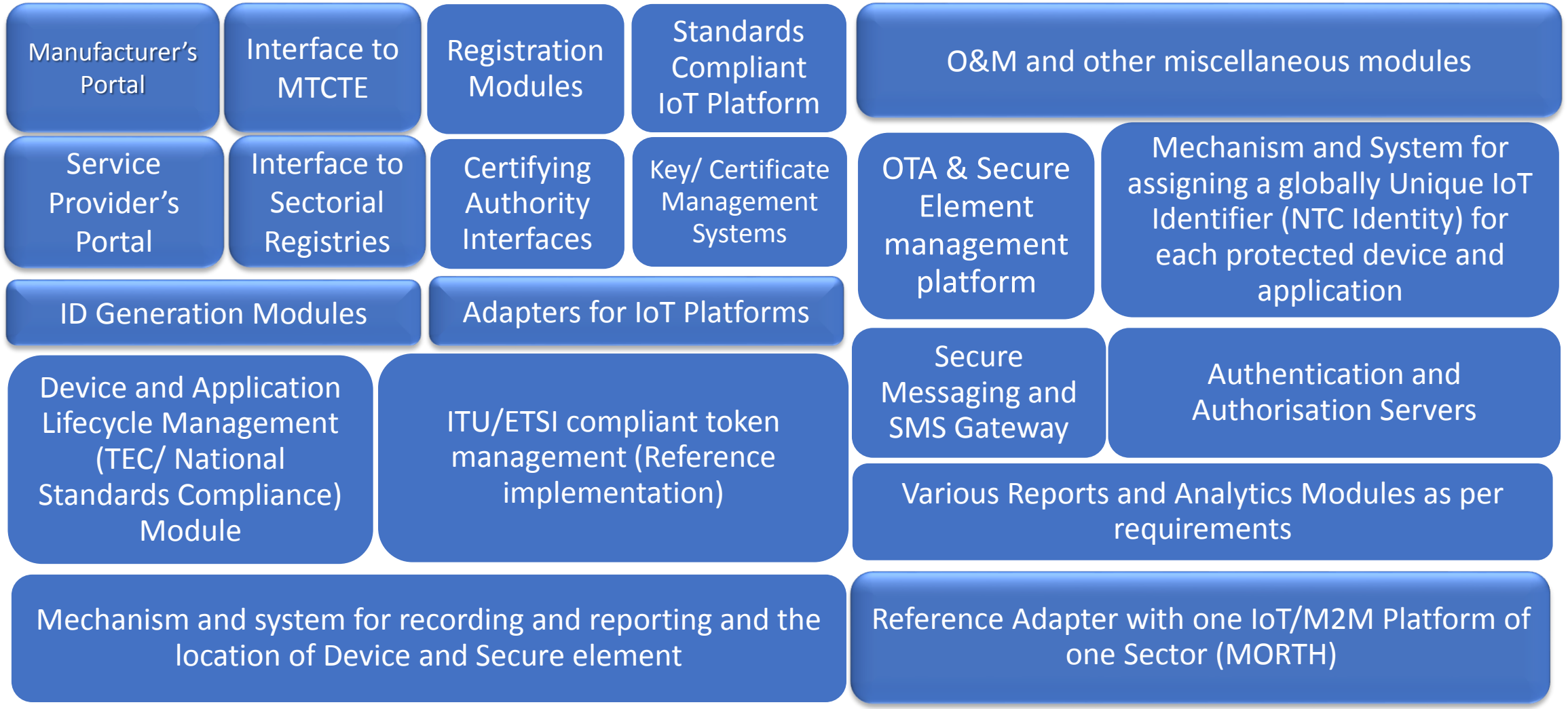
Significant efforts of standardization would be required along with enforcement of Policies

Scope for NTC

- Interfaces for the registration of Device Manufacturers, Application Providers, Platform Providers, Connectivity Providers, Application Service Providers etc.
- Interfaces which can be used by the manufacturers for registering the IoT/M2M devices (which are capable of communicating over a network) using a unique identifier.
- Interfaces for MTCTE portal using which the security label of a device along with the test results would be notified for the devices.
- Interfaces for Application registration and provisioning of unique App-ID
- This registry shall be used as an enrolment platform which may allow/prohibit the device/application from getting onboarded.
- Development of adapters to interface with the sectorial platforms and registries.
- Interface for integration with the pki framework of Government of India
- Interfacing with Global Black-List/White-List of devices would be an optional feature.
- Query Engine and Generation of Reports

Solution Components of NTC From C-DOT

The following solution components shall be provided by C-DOT



Thanks