VIRTUAL CONFERENCE

SMART CITIES INDIA 2021

7TH EDITION

26th August 2021 ⚙ 1000 - 1600 Hrs (IST)

Session: Digital Transformation of Indian Cities Towards Smarter, Sustainable & Safer Future

Securing Smart Cities: Standards and Best Practices

By

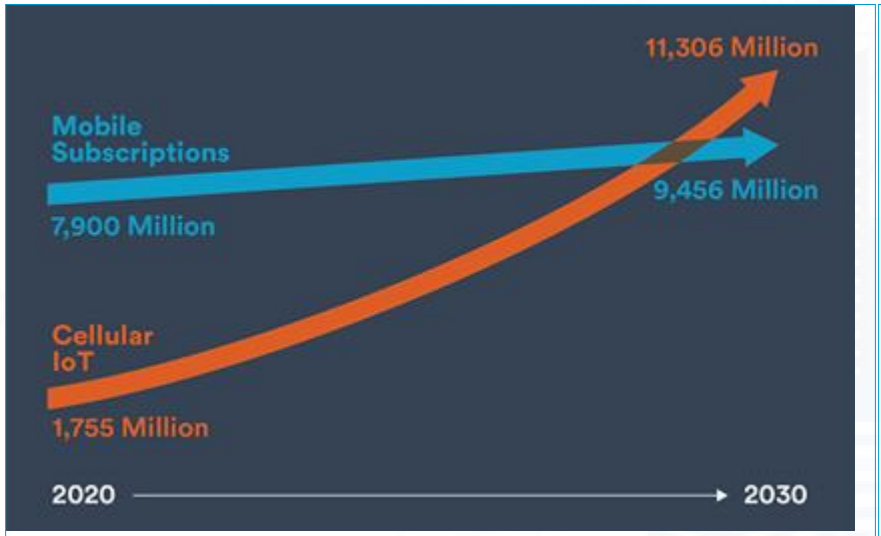
Sharad Arora

Founder & MD, Sensorise Digital Services,
Vice Chair, SGSS & GC member, TSDSI

Securing SmartCities: Importance of Standards, Interoperability and Platforms

- Security, Trust, Trusted ICT infrastructure
- Vulnerabilities, Threats and Trust Index
- Imperatives for securing the Ecosystem - Root of Trust, Security by Design, Data Security, Common Service Layer Platform
- Indian Standards for SmartCities
- Summary and Close

Technology is evolving rapidly, business models are changing by the day



Ref: Beecham Research

We are now in the age of intelligent connectivity, where the device must choose automatically from one amongst various connectivity options

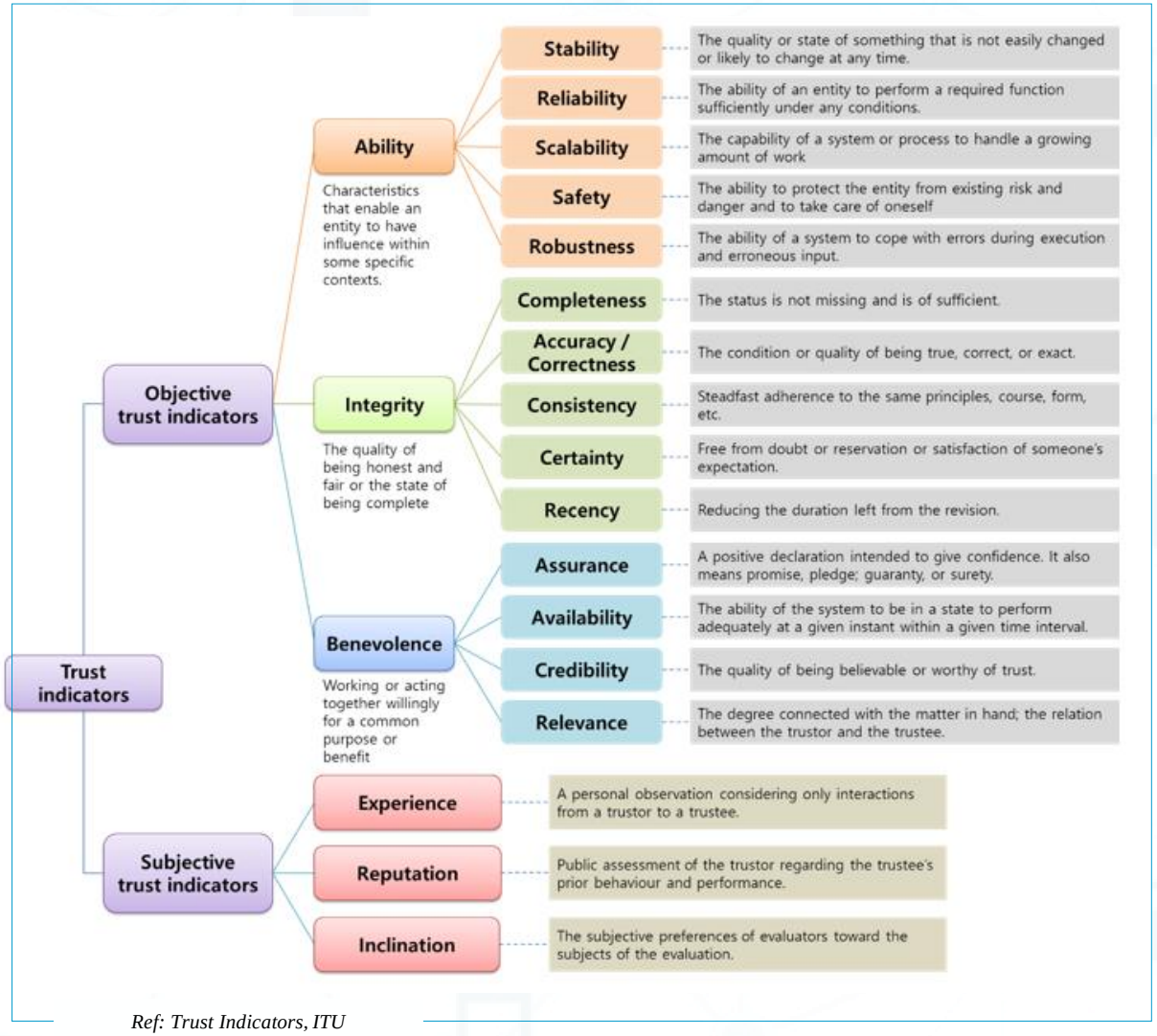
Candidates for Private Cellular Networks

Manufacturing	Predicting supply chain incidents by analysing dependencies Predictive maintenance to avoid breakdowns Improving market positioning of products through identifying customer preferences Process monitoring to detect trends in order to react to changes Agglomerating global data to detect industry trends
Healthcare	Predicting likelihood of hospital readmission through remote monitoring of patient status Optimising resource allocation for treatment Predicting diagnosis Traceability in drug manufacturing and distribution to assure transparency
Transport & logistics	Optimising container tracking and storage Vehicle tracking to minimise costs, fuel usage and speed up delivery
Agriculture	Remote monitoring of animal assets to optimise care Remote monitoring of soil properties to optimise yields
Retail	Analysing customer behaviour to reduce churn Increasing sales through targeted marketing

IoT Use Cases

Who to Trust! What to Trust?

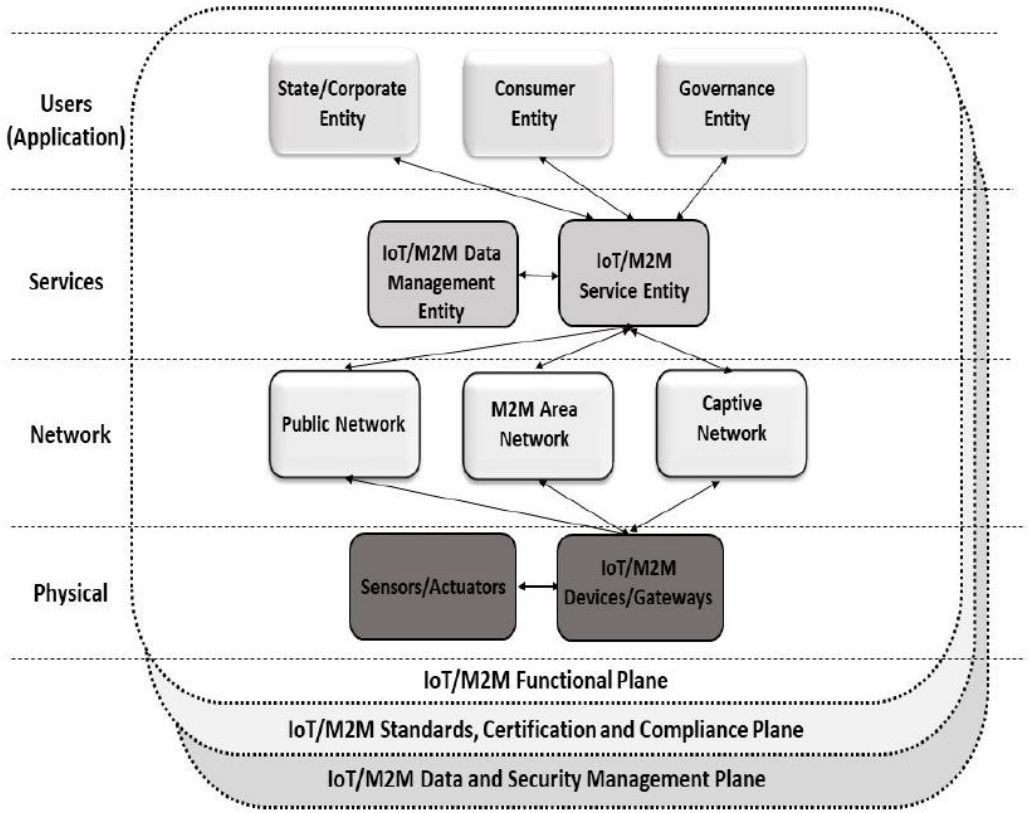
“On the Internet, nobody knows you`re a dog”



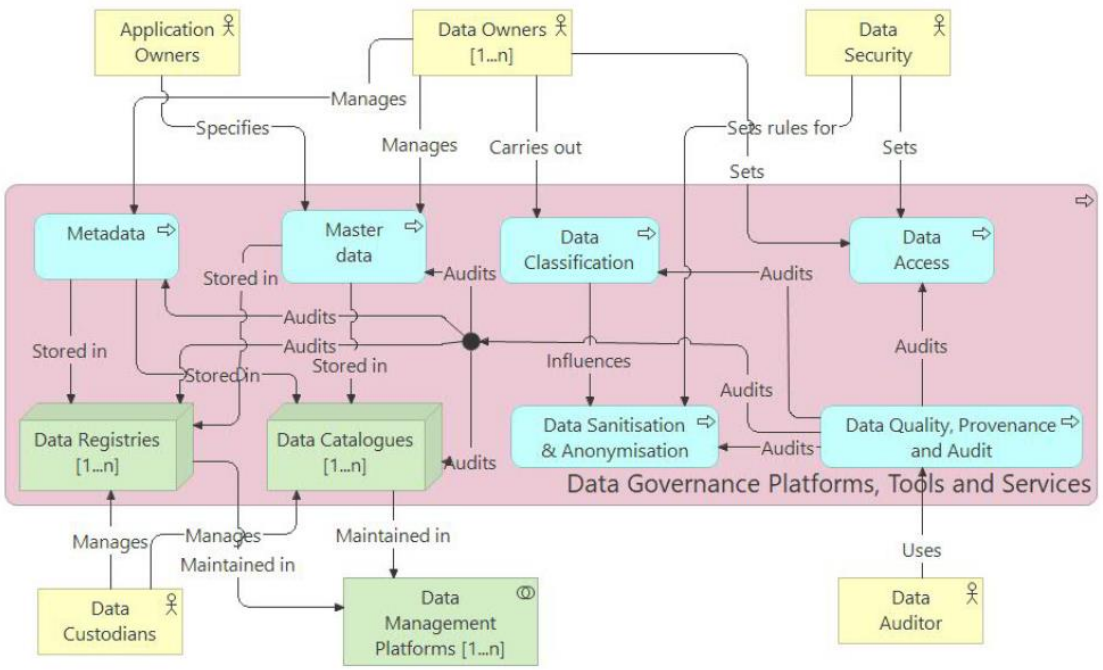
Ref: Trust Indicators, ITU

Securing the national digital infrastructure is critical for orderly growth and proliferation of the high tech capabilities

BIS ICT and IoT Reference Architecture



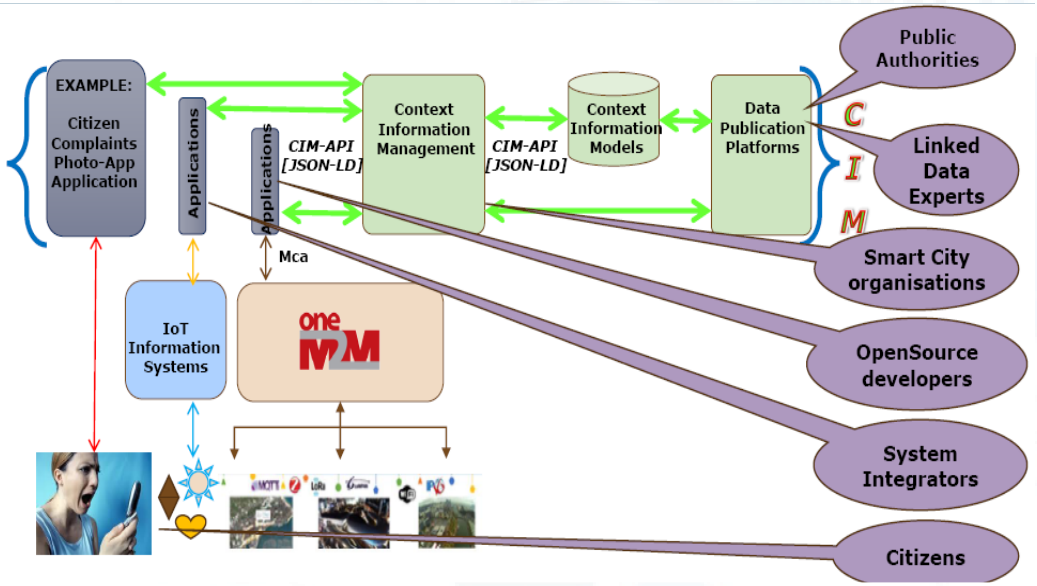
Ref: Entity based IoT Reference Model, IS 18004 (Part 1) : 2021



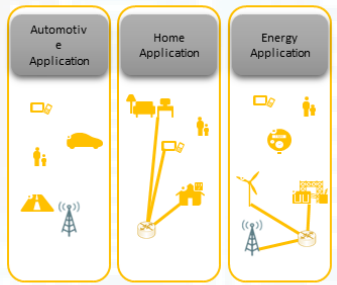
Ref: Data Governance Process, Tools and Services, Unified Digital Infrastructure - ICT Reference Architecture (UDI-ICTRA), IS 18000 : 2020

Imperatives for IoT Data Security

Data Sharing and Inter-operability Architecture

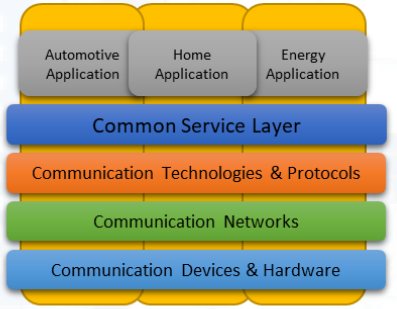


Common Service Layer Architecture



Legacy Solutions are Technology Verticals (Zigbee, DLMS for smart meters, etc.)

Disparate Machines and Applications



Horizontal framework, APIs, Objects as Resource Access Control Policy

OneM2M Common Framework

IoT Ontologies (formal description of concepts and relationships, e.g. W3C Semantic Sensor Network) as well as big data frameworks

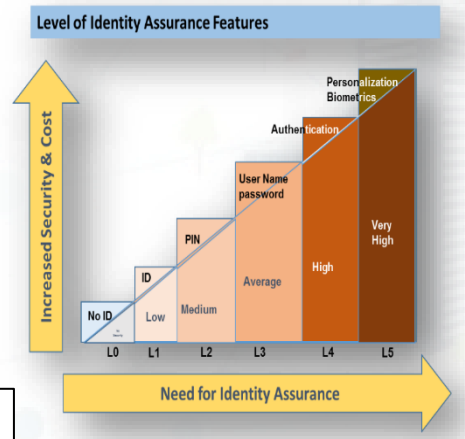
IoT Ready Ecosystem

IS_No	Title
IS 18002-1:2021	Unified Digital Infrastructure Data Layer Part 1 Reference Architecture
IS 18003-2:2021	Unified Data Exchange Part 2 API specifications
IS 18004-1:2021	IoT System Part 1 Reference Architecture

Ref: Telecom Engineering Centre Technical Report, M2M Security

Imperatives for Device and App Security

Device Security Classes



Root of trust

Registration & Certification

Trust Framework
- Unique Identity of Devices and Apps
- Keys & Certificates
- Registration of Service Providers
- Certified Devices & Applications
- Privacy Controlled Access

Identity & Authentication

Controller of Certification Authority

Use Case Classification and Compliance

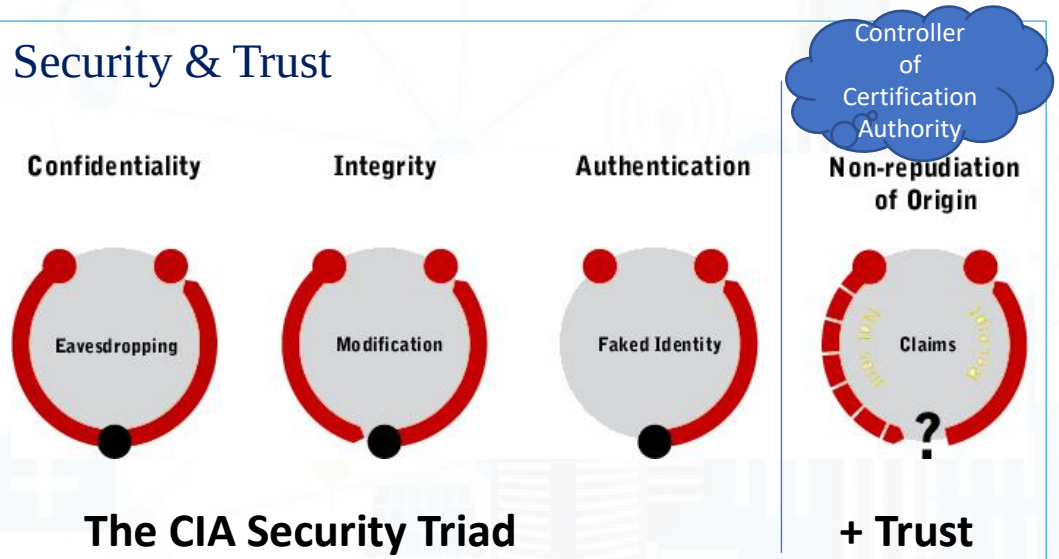
Use Case Class	Availability / QoS	Authentication Level	Encryption	KYC	
			Transport Layer	Machine	User
CQS	High	5	Mandatory	Mandatory	Mandatory
CQN	High	3		Mandatory	
CBS	Medium	5	Mandatory	Mandatory	Mandatory
CBN	Medium	2		Mandatory	
NQS	High	4	Mandatory	Mandatory	Mandatory
NQN	High	1		*	
NBS	Low	4	Mandatory	Mandatory	Mandatory
NBN	Low	0		*	

Security by Design: Unique global tamper resistant identity as **root of trust**, certification, digital trust and compliance

Ref: Telecom Engineering Centre Technical Report, M2M Security

Security, Trust, Trusted ICT infrastructure

Security & Trust

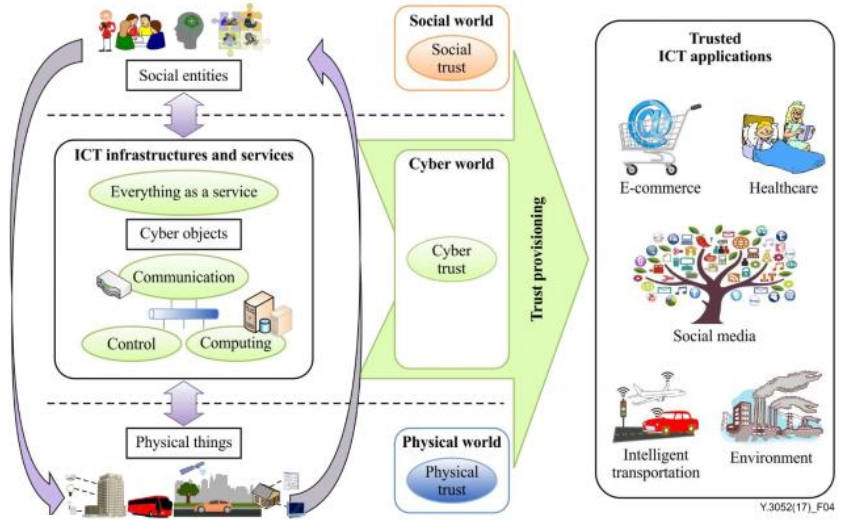


Trustworthiness Attributes

Trustworthiness	Attributes
Ability/ capability	Stability
	Reliability
	Scalability
	Safety
	Robustness
Integrity/ Honesty	Accuracy/ Correctness
	Consistency
	Certainty
	Recency
Benevolence/ Cooperation	Assurance
	Credibility
	Relevance
	Availability
	Cooperation

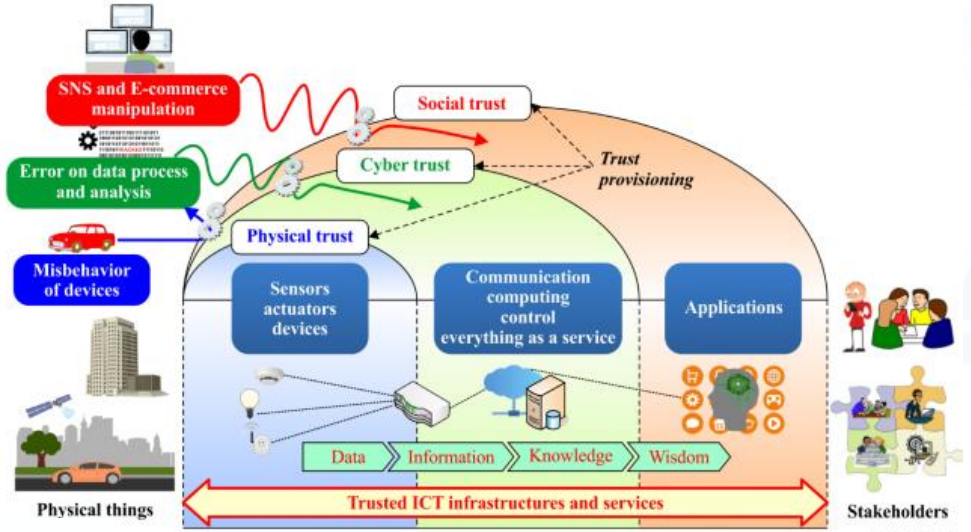
Ref: ITU-T Y.3052

Trust Domains



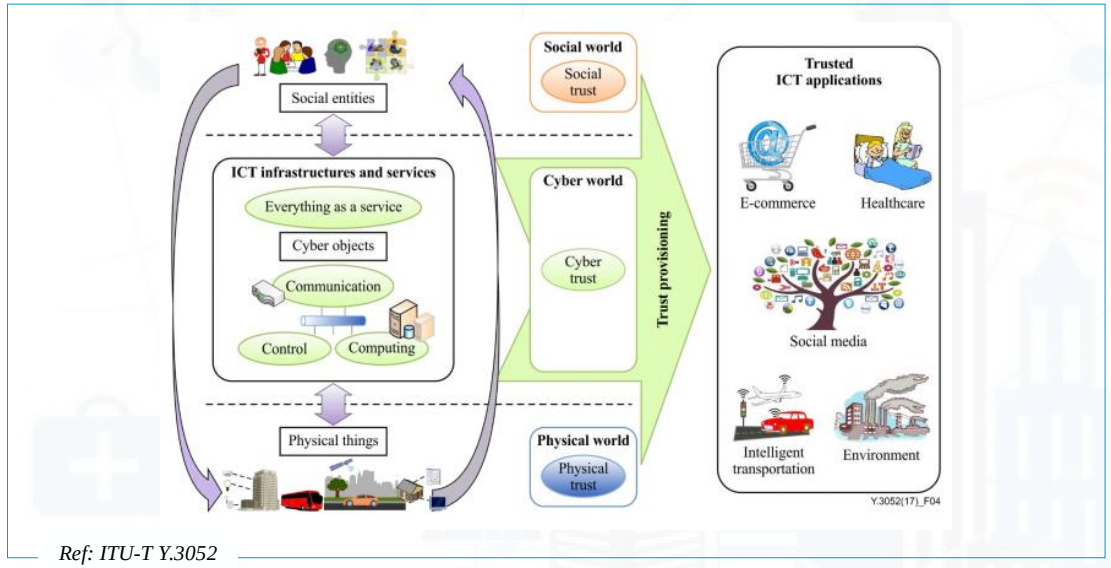
Ref: ITU-T Y.3052

Trusted ICT infrastructures

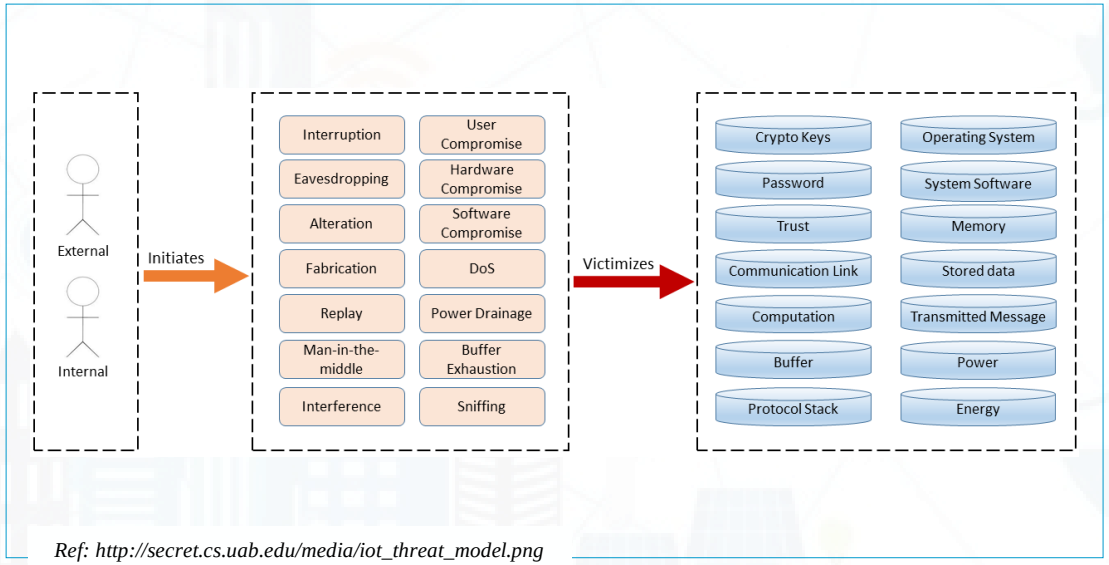


Ref: ITU-T Y.3053

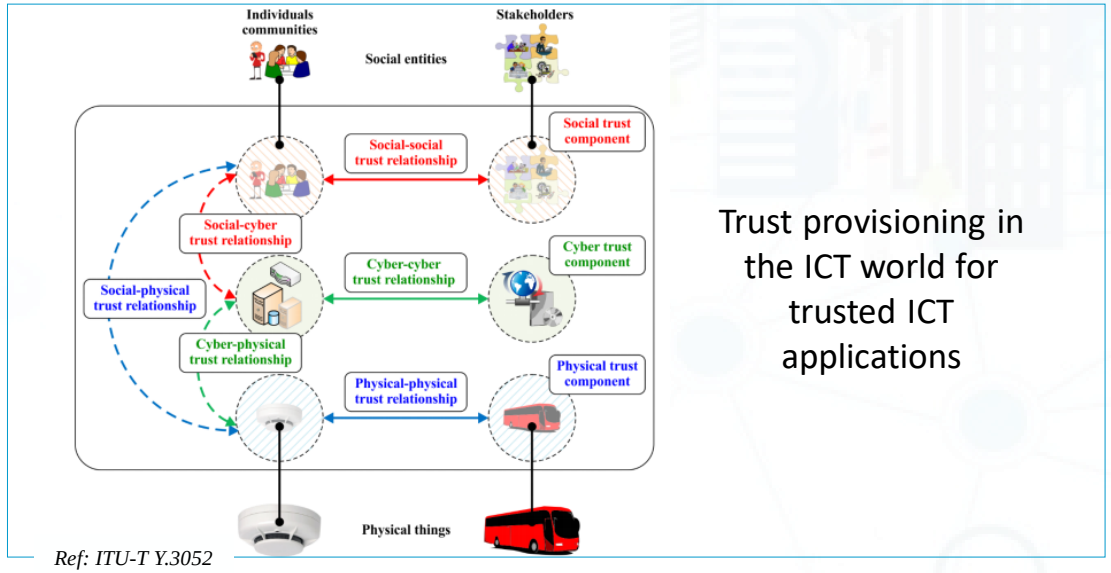
Trust Domains, Threats, Trust Index, Controls



Ref: ITU-T Y.3052

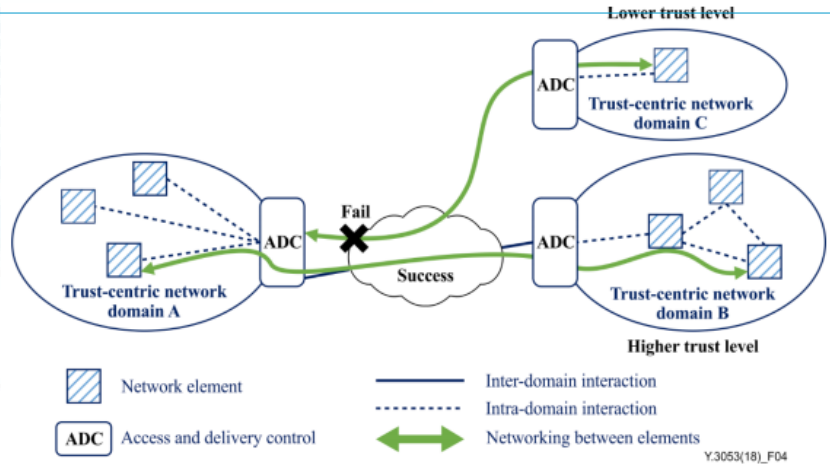


Ref: http://secret.cs.uab.edu/media/iot_threat_model.png



Ref: ITU-T Y.3052

Trust provisioning in the ICT world for trusted ICT applications



Ref: ITU-T Y.3053

Trust-centric network domains can limit access to trusted devices and applications based on trust index

oneM2M is an IoT Standards power house

Rel-1 Features

- Registration
- Discovery
- Security
- Group Mgmt.
- Data Mgmt. & Repository
- Subscription & Notification
- Device Management
- Communication Mgmt.
- Service Charging
- Network Service Exposure
- App & Service Mgmt.
- HTTP/CoAP/MQTT Bindings

Rel-2 Features

- Time Series Data
- Flexible resources that can be customized by app developers
- Semantics Description & Discovery
- Security Enhancements
  - Dynamic Authorization
  - Content Security
  - E2E Security
- WebSocket Binding
- Ontology for Home Area Information Model
- oneM2M App-ID Registry
- oneM2M Interworking
  - LWM2M
  - AllJoyn
  - 3GPP Triggering

Rel-3 Features

- Semantic Querying/Mashups
- 3GPP SCEF Interworking
  - Non-IP Data Delivery,
  - UE Reachability Monitoring
  - Device Triggering
  - Etc.
- Transaction Management
- Service Layer Routing
- Common oneM2M Interworking Framework
  - OCF, OPC UA, OSGi, Modbus
- oneM2M Conformance Tests and Profiles
- Security Enhancements
  - Distributed Authorization, etc.
- Ontology-based Interworking

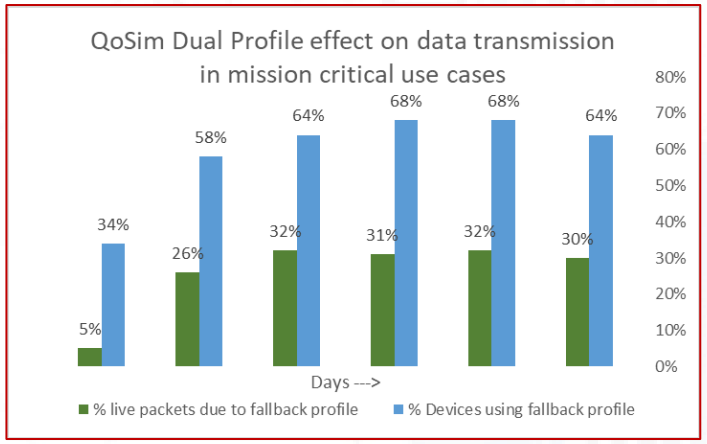
- TEC has adopted oneM2M Standards as National Standards for India https://www.tec.gov.in/pdf/M2M/M2M_TR_TS.pdf
- Standards compliance is very important for a global play for make-in-India
- Investments are required in local Test Houses, Trial Labs and Certification Labs

S. No.	Title	oneM2M TS	TSDSI Standard number
1	Functional Architecture	TS-0001	TSDSI STD T1. oneM2M TS-0001-3.15.1 V1.0.0
2	Requirements	TS-0002	TSDSI STD T1. oneM2M TS-0002-3.1.2 V1.0.0
3	Security Solutions	TS-0003	TSDSI STD T1. oneM2M TS-0003-3.10.2 V1.0.0
4	Service Layer Core Protocol	TS-0004	TSDSI STD T1. oneM2M TS-0004-3.11.2 V1.0.0
5	Management Enablement (OMA)	TS-0005	TSDSI STD T1. oneM2M TS-0005-3.5.1 V1.0.0
6	Management enablement (BBF)	TS-0006	TSDSI STD T1. oneM2M TS-0006-3.6.2 V1.0.0
7	CoAP Protocol Binding	TS-0008	TSDSI STD T1. oneM2M TS-0008-3.3.1 V1.0.0
8	HTTP Protocol Binding	TS-0009	TSDSI STD T1. oneM2M TS-0009-3.2.1 V1.0.0
9	MQTT protocol binding	TS-0010	TSDSI STD T1. oneM2M TS-0010-3.0.1 V1.0.0
10	Common Terminology	TS-0011	TSDSI STD T1. oneM2M TS-0011-3.0.1 V1.0.0
11	Base Ontology	TS-0012	TSDSI STD T1. oneM2M TS-0012-3.7.3 V1.0.0
12	LWM2M Interworking	TS-0014	TSDSI STD T1. oneM2M TS-0014-3.1.1 V1.0.0
13	Secure Environment Abstraction	TS-0016	TSDSI STD T1. oneM2M TS-0016-3.0.2 V1.0.0
14	WebSocket Protocol Binding	TS-0020	TSDSI STD T1. oneM2M TS-0020-3.0.1 V1.0.0
15	Field Device Configuration	TS-0022	TSDSI STD T1. oneM2M TS-0022-3.0.1 V1.0.0
16	Home Appliances Information Model and Mapping	TS-0023	TSDSI STD T1. oneM2M TS-0023-3.7.3 V1.0.0
17	OIC Interworking	TS-0024	TSDSI STD T1. oneM2M TS-0024-3.2.2 V1.0.0
18	3GPP Interworking	TS-0026	TSDSI STD T1. oneM2M TS-0026-3.0.0 V1.0.0
19	Ontology Based Interworking	TS-0030	TSDSI STD T1. oneM2M TS-0030-3.0.2 V1.0.0
20	Feature Catalogue	TS-0031	TSDSI STD T1. oneM2M TS-0031-3.0.1 V1.0.0
21	MAF and MEF Specification	TS-0032	TSDSI STD T1. oneM2M TS-0032-3.0.0 V1.0.0
22	Interworking Framework	TS-0033	TSDSI STD T1. oneM2M TS-0033-3.0.0 V1.0.0
23	Semantics Support	TS-0034	TSDSI STD T1. oneM2M TS-0034-3.0.1 V1.0.0
24	OSGi Interworking	TS-0035	TSDSI STD T1. oneM2M TS-0035-3.0.0 V1.0.0
25	Use Cases Collection	TR-0001	TSDSI STD T1. oneM2M TR-0001-3.1.1 V1.0.0
26	Vehicular Domain Enablement	TR-0026	TSDSI STD T1. oneM2M TR-0026-3.0.1 V1.0.0
27	Study on Enhanced Semantic Enablement	TR-0033	TSDSI STD T1. oneM2M TR-0033-3.0.0 V1.0.0

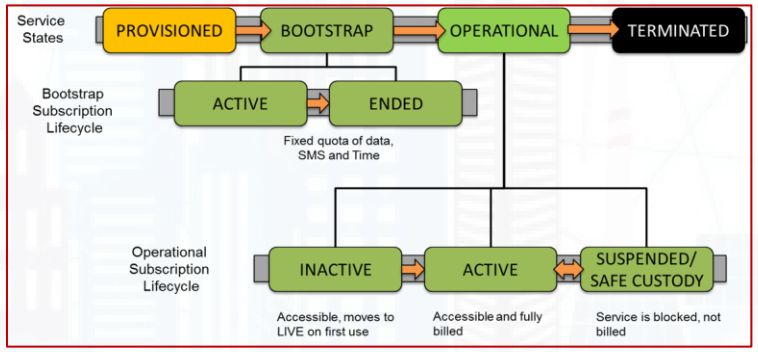
TSDSI Transposed oneM2M Release 3 standards

TEC ESIM Standard has made available frugal and high QoS connectivity for devices

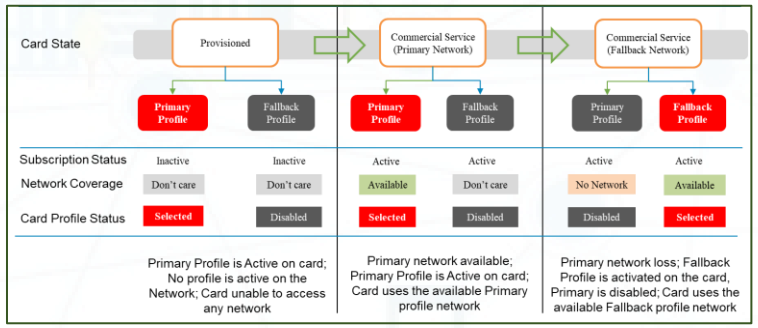
- Multi-network QoS for mission critical use cases,
- Frugal remote manageable M2M connectivity, choice of Domestic and International Networks
- Single Dashboard and Self Care platform, supporting multiple MNO subscriptions



Mission Critical quality of service with dual network profile



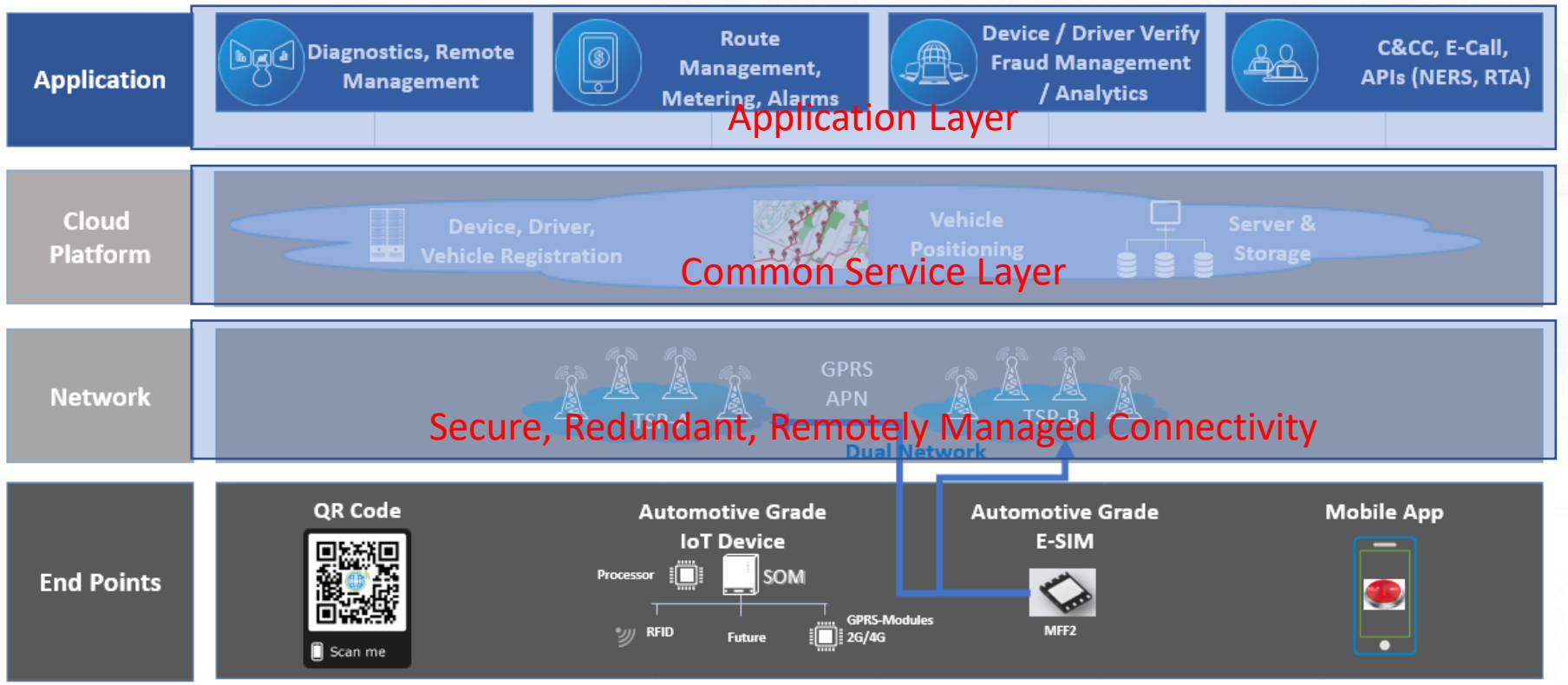
Connectivity Lifecycle management through multiple device lifecycle stages



Flexible, frugal, secure and remote manageable M2M Connectivity for all Smart Cities Use cases

Securing Public Transport – Nirbhaya Framework

ESIM as a root of trust, Common Service Layer as the Trust Infrastructure



Ref: Sensorise contribution to Architecture for Public Service Vehicle Tracking Architecture for AP State

AIS140
IS 16833 : 2018 Automotive Tracking Device (ATD) and Integrated Systems

AIS140 / BIS 16833 Standard

BSNL
Connecting India

The AIS140 Standard/ Nirbhaya framework has created an open ecosystem of more than 200 MSMEs offering devices, applications and IoT connectivity, BSNL provides the National Backend that hosts public service vehicle data

Summary

1. Government spending and impetus is critical to developing high tech services and solutions, 100 Smart Cities is an important initiative of the government to drive this objective of national capability development. Indian contributions to global standards are critical for local capability development, IPR creation for which, registration and recognition of IoT/ M2M MSMEs as Service and Solution Providers is critical to the orderly development of the ecosystem [M2M Service Provider regime]
2. Standards Development Organisations (SDOs) such as BIS and TSDSI, are working very hard to bring cutting edge standards to India, Digital Standards Setting Organisation, Telecom Engineering Centre, has adopted many global standards as National Standards over the last two years which directly assist SmartCities ICT infrastructure
3. SmartCities must define its ICT specifications as per the National Standards, such that an interoperable, scalable, trustful and globally competitive infrastructure is first deployed in the country, and then replicated in other parts of the world
4. SmartCities procurement policies must keep in mind the critical importance of Make-in-India, Digital India and Start-Up India along with the provisions of the Preferred Market Access and Production Linked Incentives announced by Ministry of Commerce
5. Use of Indian Local Certification capabilities, Local Test Houses and Local New Technology Labs (e.g. 5G labs) are critical for enabling the local innovation from MSMEs in IoT/ M2M/ICT domain. Certification is required not just for Products but also Services and Use Cases; use of Indian Root Certification infrastructure is critical for security and control
6. The Indian Government, SDOs, SSOs, Academic Institutions, R&D Institutions must work hand in hand with the Industry to create a global standards backed vibrant SmartCities ecosystem in India in 2021 and beyond

Thank You

sharad.arora@sensorise.net
9212109999
skype: sharad.arora
linkedin.com/in/sharadsan

Sensorise Digital Services, Sharad Arora

Speaker Profile

- Mr. Sharad Arora is an Engineer by profession and has more than 31 years of experience in broad range of leadership roles across various spheres of IT and Telecommunication Services.
- As a telecom industry professional, he has played a major role in setting up of green field IT and Network operations for a GSM operator and the launch of the 3G business with a huge portfolio of enterprise and lifestyle products such as a mobile wallet, surveillance, school bus tracking, security etc.
- Sharad is a visionary thinker with a global perspective, great leadership abilities, technical skills, learnability, focus and perseverance for successful orchestration of complex and large scale "idea to standard" programs. He is a technology evangelist and holds deep expertise in the areas of Telecom technologies & Operator IT and BSS, Certification Authority Technologies and Deployment, Network and Device Security, Machine to Machine Communications, Embedded Systems and IoT, IT for Telecom VAS, SIM cards, related infrastructure and security.
- As Vice Chair, SGSS & Governing Council member, TSDSI, he has continuously supported the standardization and policy initiatives for Telecom, IT, Transport and Urban Development. His valued contributions as an author/ editorial member enlist more 6 Technical Reports, 2 ITU contributions and several TSDSI initiatives other than being an active member of three National Working Groups, BIS Sectoral Committee on IoT, Niti Aayog Telematics Committee, TSDSI Roadmap and Outreach Committee.

Company Profile

- Sensorise is a role model Internet of Things (IoT) and Machine to Machine (M2M) service provider and a licensed VNO, with expertise in supplying end-to-end frugal business solutions for improving Quality of Service (QoS), remote management and lifecycle management of M2M and IoT Devices.
- As an industry leader, Sensorise contributes to responsible and orderly growth of IoT and M2M domain, bridging the gaps in infrastructure, technology and services with responsible contribution to standards, policies & regulations to build compliant ecosystems for consumers, partners and governments.
- Sensorise solutions offer dispersed assets, remote management, high QoS M2M connectivity and complete security in the IoT/M2M domain. Sensorise is credited to bring the very first factory ready machine solderable ESIM in India. Characterized by a unique proposition for multi-network remotely manageable connectivity, Sensorise offers exclusive QoSim and SenseLCM products under IOT/M2M services.
- Awarded with the 'Best IoT Service Provider' at ET Telecom awards 2020, also the recipient of the 2019 International Stevie Bronze Award, Vienna in the category of the Most Innovative Telecom Service Provider for its 'End to End Connectivity Service Provider for Machine Critical Use Case (IoT/ M2M)' – just to name a few.