TELECOMMUNICATION ENGINEERING CENTRE

दूरसंचार अभियांत्रिक केन्द्र

MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY

संचार एवं सूचना प्रोद्योगिकी मंत्रालय

DEPARTMENT OF TELECOMMUNICATIONS

दूरसंचार विभाग

GOVERNMENT OF INDIA

भारत सरकार

सत्यमेव जयते

ISO 9001:2008

IOT SECURITY -WORKS AT TEC

From: SHAILENDRA K SHARMA
DDG Smart Networks, TEC
Email: shailendrak.sharma@gov.in
Mobile: +91-9013135311

27-08-2019

Background of M2M Working Group –Security (Contd.):

- The work of M2M Security working group was **to Smart Network (SN) division, in Nov 2016.**
- The working group was reconstituted with some additional members.

- A **Face to Face (F2F) meeting of the M2M Security Group (SG) held on 22-02-2017** to formulate further work plan

- Meeting received wide participation from various sectors of industry.

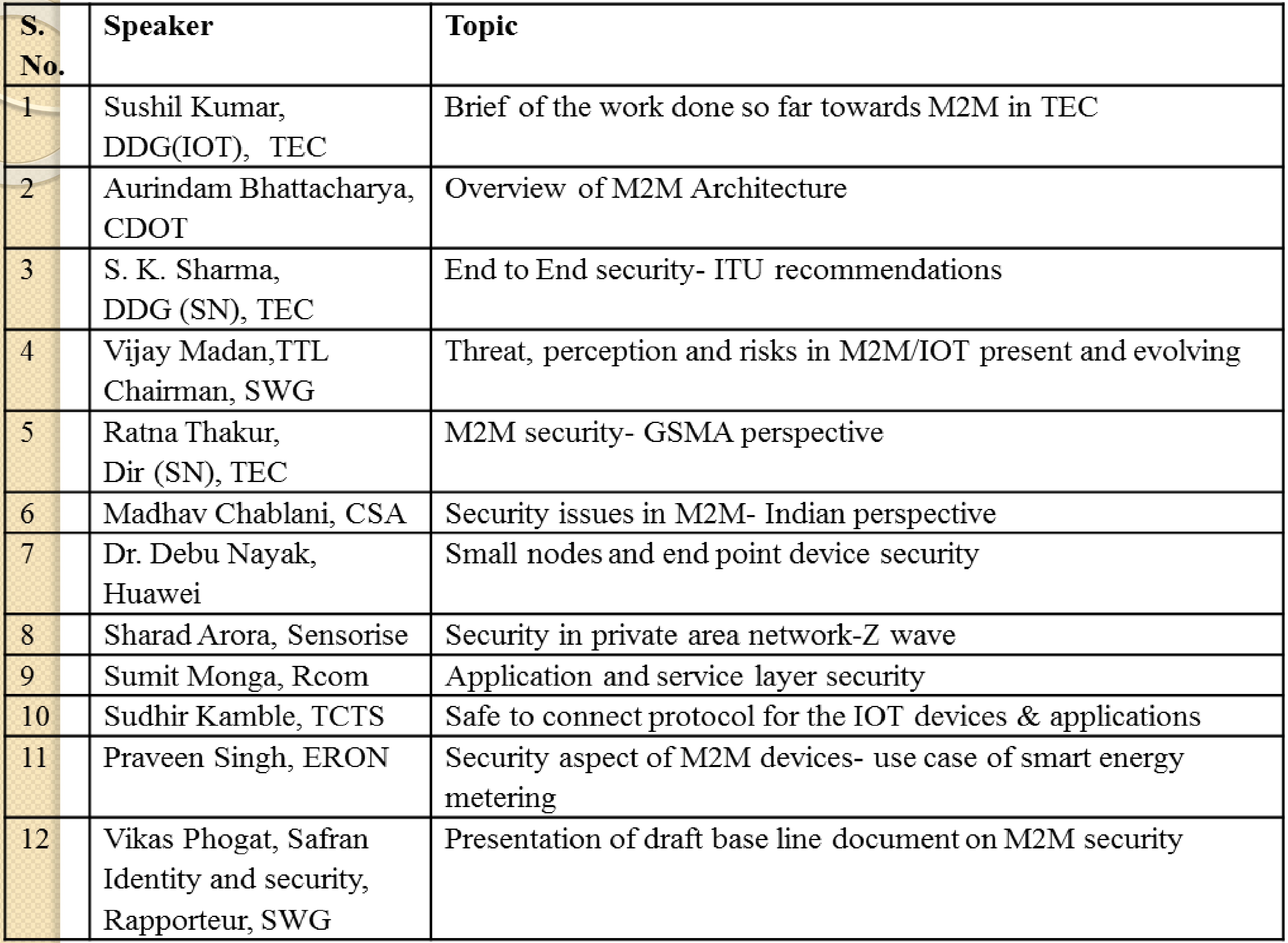
- **More than 40 Intelligentsia** from various industries / organisations related to M2 M participated in the meeting

Salient points discussed in Meeting dated 22nd Feb 2017

- Deliberations were made on various aspects of M2M security including following:
  - various aspects of security in Telecom
  - Brief **overview of M2M**
  - **Security** concerns in the area of M2M
  - **Threat perceptions** for M2M
  - **End point device security** etc.
  - presentations were made on security aspects in IoT/M2M.

Salient points discussed in Meeting dated 22nd Feb 2017(contd.)

Presentations given in the meeting:



S. No.	Speaker	Topic
1	Sushil Kumar, DDG(IOT), TEC	Brief of the work done so far towards M2M in TEC
2	Aurindam Bhattacharya, CDOT	Overview of M2M Architecture
3	S. K. Sharma, DDG (SN), TEC	End to End security- ITU recommendations
4	Vijay Madan,TTL Chairman, SWG	Threat, perception and risks in M2M/IOT present and evolving
5	Ratna Thakur, Dir (SN), TEC	M2M security- GSMA perspective
6	Madhav Chablani, CSA	Security issues in M2M- Indian perspective
7	Dr. Debu Nayak, Huawei	Small nodes and end point device security
8	Sharad Arora, Sensorise	Security in private area network-Z wave
9	Sumit Monga, Rcom	Application and service layer security
10	Sudhir Kamble, TCTS	Safe to connect protocol for the IOT devices & applications
11	Praveen Singh, ERON	Security aspect of M2M devices- use case of smart energy metering
12	Vikas Phogat, Safran Identity and security, Rapporteur, SWG	Presentation of draft base line document on M2M security

- The roadmap for preparation of security document was discussed

- It was decided that for smooth functioning study area would be divided
- into **further five sub –groups**:

Sub-Group	**LPCC(Lead Person Cum Co-ordinator)**
• **Sub group 1 : End Point Devices Security:**	**Sh. Vikas Phogat (Pranav Singh)**
• **Sub group 2 : Network Communication Security:**	**Sh. Sumit Monga**
• **Sub group 3 : Application Level Security:**	**Sh. Sharad Arora**
• **Sub group 4 : Trusted Environment Security:**	**Sh. Vijay Madan**
• **Sub group 5 : Service Layer Security:**	**Sh.Aurindam Bhattacharya**

Workgroup and Work Process

- The Sub-Groups worked in closed co-ordination within the SG as well as across the sub-groups to study the topic assigned to them and prepare the recommendations.
- The LPCCs continuously shared their progress and feedback through audio conferencing as well as face to face meetings.
- Secretariat at TEC of following officers played a Key role in compilation and finalization of the TR
- Director SN Ms Ratna Thakur
- ADG SN Sh Manish Ranjan

Points kept in view while preparing of report

ISO 9001:2008

The report has been prepared keeping in view the following guiding factors:

- The SG feels that M2M Security WG Recommendations shall not aspire to be a standard

- The report should rather act as a guideline that prompts the use of appropriate standards in Policy Making and Deployment and shall act as guiding document for:
  - **The Industry that hopes to be benefited from the large opportunity of M2M/IoT**
  - **The Government Policy makers who must act in the interest of the enablement of Indian Industry to develop products and solutions that can capture the global marketplace.**
  - **The End User and Industrial User of the new M2M/IoT Applications, whose safety, ease-of- use and interests must be safe-guarded.**

Many use cases have been incorporated as examples for the level of security required in each case.

Compilation of report document and Circulation

ISO 9001:2008

- The document was compiled and circulated to all WG members vide mail on 1st March 18.
- Members were requested to send the feedback by 10th March 18.
- The feedback received were discussed on audio conference meeting dated 12th march 18.
- In the audio conference, the queries raised were answered by LPCCs
- The feedback received was incorporated in the draft
- The draft report circulated on 15th March to all members

Transparent and Democratic Approach in Building the Document

- The draft report again circulated to all LPCC's in April , June 2018 followed by PP on 21-8-18 in TEC and circulation of SWG report on 4th Sep 2018 after inclusion of feedback
- F2F meetings on 19th Sep, 16th Oct, 27th Nov 2018, and a final Review meet in Dec 2018 for Finalisation of TR on IOT Security.
- TR, by the, of the,for the People (Society)Approach.

Release of the TR on Recommendations for IOT / M2M Security

- TR on Recommendations in IOT Security released on 8th January 2019 by Hon’able Minister of State (Independent Charge) for Communications and MoS for Railways, Govt of India Sh Manoj Sinha,

What is IOT

- The internet of things (IoT) is a computing concept that describes a scenario where everyday physical objects are connected to the internet and can identify themselves to other devices or processes, **via an IP addres**
- **The IoT is significant because an object that can represent itself digitally becomes something greater than the object by itself.** No longer does the object just relate to the process; it now connects to surrounding objects and database data, permitting "big data" analytics and insights.

Contd

- In particular, “things” might communicate autonomously with other things and other devices, such as sensors in manufacturing environments or an activity tracker with a smartphone.
- IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems, **microservices** and the internet
- This convergence has torn down the walls between operational technology and information technology, allowing unstructured machine-generated data to be analysed for insights that will drive improvements

IoT/M2M Communications

- From the operational perspective, smart devices can communicate via several models, such **as device-to-device** This is where two or more devices can directly communicate with each other through various network protocols, including internet protocol (IP), Bluetooth, Z-Wave or ZigBee. This type of protocol is typically used with **low data rate requirements** such as light bulbs, light switches and door locks

IoT/M2M Communications

- Another way of communicating is by **device-to-cloud.** An IoT device connects directly to an internet cloud service to exchange data. It typically uses wired Ethernet of Wi-Fi connections between the device and the IP network. This type of connection is used by Smart TVs

IoT/M2M Communications

- **Device-to-gateway** is a method where the device connects through an application-layer gateway as a conduit to reaching a cloud service. The gateway provides security and other functionality such as protocol translation. A typical use is a **smartphone running an app to communicate with a device, such as a fitness band, and relay data to a cloud service.**

IoT/M2M Communications

- Finally, **back-end data sharing refers to a communications architecture that enables users to export and analyse smart object data from a cloud service in combination with data from other sources.** The back-end sharing architecture allows the data collected from a single IoT device data streams to be aggregated and analysed.
- Smart devices have used internet protocol, **IPv4, that is running low on available IP addresses**. This is being replaced by IPv6 that will provide sufficient IP address possibilities for the foreseeable future

IoT/M2M Communications:

- The Internet of Things (IoT) refers to the use of intelligently connected devices and systems to leverage data gathered by embedded sensors and actuators in machines and other physical Objects / Things. M2M is a subset of IoT.

- Machine to Machine communications, often termed M2M/IoT is going to be the next generation of Internet revolution connecting more and more devices on Internet.

- M2M communications refer to automated applications which involve machines or devices communicating through a network without human intervention.

- Sensors and communication modules are embedded within M2M devices, enabling data to be transmitted from one device to another device through wired and wireless communications networks.

- M2M is expected to revolutionize the performance of various sectors, businesses and services, by providing automation and intelligence to the end devices, in a way that was never imagined before.

IoT/M2M Communications

- For further detailed information inquisitive reader may consult TR on M2M communications, recently brought out by TEC

What is security?

- As per Wikipedia, **Security** is freedom from, or resilience against, potential harm (or other unwanted coercive change) from external forces. Beneficiaries (technically referents) of security may be persons and social groups, objects and institutions, ecosystems, and any other entity or phenomenon vulnerable to unwanted change by its environment.

- From the above definition, we can say that ensuring security needs:

1. Knowing external sources, which can potentially harm and entity
2. Taking corrective measures to ensure freedom from these sources

Need for security in IoT

ISO 9001:2008

- The emergence of the Internet of Things (IoT) is creating new service providers looking to develop new, innovative, connected products and services.
- hundreds of thousands of new IoT services connecting billions of new IoT devices over the next decade is expected(275 million device in India by 2020)
- 25 Billion IoT devices expected by 2020
- security issues are significant inhibitor to the deployment of many new IoT services
-

- Challenges in IoT security:

- Since IoT exposes private information of individuals to Wide Area Network, it is more prone to frauds.
- Security comes at a **cost**

- Many a times, the devices are **low cost, low power devices**

- The **investment in security cost may not appear to be economical for the low cost devices**.
- **Balancing the cost vs need for security** is the factor determining the level of security for the device

Trusted Environment for M2M / IoT Security

Trusted Environment, enhanced security and Data Privacy

- **Mass proliferation of M2M & IoT** , Billions of devices
- Each operation and communication of connected devices in the form of action , interaction, transaction, transfer, processing online etc. activities, leave behind detailed footprints
- Equally important - besides the connected devices, security of applications and services also taken seriously
- Trust environment a challenge – Devices Scattered, Multiplicity of Types, proprietary standards, variety of use cases, different types of connectivity, end to end processes

Trusted Environment, enhanced security and Data Privacy

- End to end security – Nodes, Applications, Services
- **A trust and security in the end to end ecosystem by all stakeholders becomes one of the key drivers for progressive and sustained growth**.
- Trust: All actions and Actors (ASSETS) - Behave as per expected behavior
- Disruptions – Threats – Attacks – Breaches , tend to shake confidence and trust
- Untrusted actions / actors to be transformed into trusted to have harmony
- Confidence and involvement of all stakeholders, users

Trust – A few Basics

- **At deeper level, trust is regarded as a consequence of progress towards security or privacy objectives.**

- Trust - **An accumulated value from history and the expecting value for future**.
- Quantitatively and/or qualitatively calculated and measured - used to evaluate values of physical components, value-chains among multiple stakeholders, and human behaviours including decision making.
- As a lexical-semantic - reliance on the integrity, strength, ability, surety, etc., of a person or object.
- A measure of confidence that an entity will behave in an expected manner, despite the lack of ability to monitor or control the environment in which it operates.

- Revolves around assurance and confidence that people, data, entities, information or processes will function or behave in expected ways.

M2M and IoT sustainability in trusted ecosystem

- Defined as sustainability, it is the risk and implications of devices, systems, nodes, back and front end platforms that are left un-patched, orphaned, or bricked which is critical to realizing the promise of IoT.
- The insertion of a smart device capable of extracting protected data or doing malicious actions which can infect the whole network with relative ease.
- Thus it becomes imperative to discover whether or not new devices have the right capabilities and compatibilities with other sensors.
- A zero knowledge protocol that achieves precisely that objective while keeping the sensor data private.

IOT-Security

- The future of IoT/M2M cannot be realized without addressing security and privacy risks and policy issues.
- Securing and protecting the things that matter most—our systems, our data, and our privacy—is a shared responsibility.
- Security and privacy must become part of every product’s feature set.

IOT-Security: Affected Stakeholders

- The Following stakeholders are affected by the IoT/M2M Security threats
- M2M Application Service Provider;
- Manufacturer of M2M Devices and/or M2M Gateways;
- M2M Device/Gateway Management entities;
- M2M Service Provider;
- Network Operator
- User/Consumer

The trust enabling architecture, zones and attributes

- Serves the purpose of establishing security and trust between all parties involved in the M2M ecosystem.
- Comprises following infrastructure functions
  - M2M Enrolment functions - managing the enrolment of M2M Nodes and M2M applications for access to M2M Services provided by an M2M Service Provider.
  - M2M Authentication functions - manage identification and authentication
  - M2M Authorization functions - handles authorization requests to access resources.
  - The above functionalities - assumed to be operated by trusted parties (generally M2M Service Providers but possibly also by trusted third parties)

oneM2M / GSMA Security specifications , reports , references

- TR-0008-V2.0.0 - TR analyses security issues , which may arise from use cases, captures relevant threats, maps them to the security requirements and derives possible security mechanisms to realize the security features for oneM2M
- TS-0026-V-0.2.0 - Specifies interworking between oneM2M service layer and 3GPP Rel-13 & Rel-14 features, to expose some 3GPP Rel13 & Rel14 features to oneM2M service layer for benefit of IoT applications, and vice-versa
- TR-0012-V2.0.0 - oneM2M End-to-End Security and Group Authentication
- GSMA Reports - CLP 1 to CLP 4
- Safe to connect protocols – Trust Protocols Processes – Zero Protocols
- TS-0003-V3.3.1 - The TS defines security solutions for M2M systems
- ITU –T Transposition of oneM2M
- Release 3 due next year

Standards and Reports – WPs and issues

- Others address key challenges of IoT Network in terms of Security, Cost, Ecosystem, Fragmentation, Coverage
- Some deal with security and privacy perspective,
  - predicted pervasive introduction of sensors and devices into currently intimate spaces – such as the home, the car and with wearables and ingestible, even the body – poses particular challenges.
- Non –observance and non-implementation of the same would be disastrous
- All above include:
  - innovation, leadership, standards and collaboration.
  - requirement of regulatory framework:
  - sound regulations;
  - good rules (including appropriately limited exceptions);
  - full and honest application and enforcement of those rules and regulations (and exceptions).

5G - Enabler of IOT

- Industry groups and institutions have identified a set of eight requirements for 5G:9
- □ 1-10 Gbps connections to end points in the field
- □ 1 millisecond end-to-end round trip delay (latency)
- □ 1000X bandwidth per unit area
- □ 10-100X number of connected devices
- □ (Perception of) 99.999% availability
- □ (Perception of) 100% coverage
- □ 90% reduction in network energy usage
- □ Up to ten-year battery life for low power, machine-type devices.

Security is the critical enabler for IoT/M2M

Constitutes the biggest Impediment to proliferation

The IoT threats are more serious, enhanced from merely manipulating information to controlling actuation.....from the digital to physical........with the possibility to cause grave consequences of public health, safety, and security

IoT requires greater security and privacy than the “virtual” internet or the “wireless” mobile

Trust

- Before we talk about security in IOT (Ecosystem , comprising various stakeholders like, device Manufacturers , TSP’s, M2M SP’s, End Users, etc) , Let us delve briefly on Trust . Trust in IOT Ecosystem.

Trust

- Definition of Trust
- Attributes of Trust
- Understanding of Trust
- Relationship between IOT security, Privacy and Trust.
- Trust in ICT Environment

ITU-Def

- **Trust: Trust is an accumulated value from history and the expecting value for future. Trust is quantitatively and/or qualitatively calculated and measured, which is used to evaluate values of physical components, value-chains among multiple stakeholders, and human behaviours including decision making.**
- NOTE 1 - Trust is applied to social, cyber and physical domains.
- NOTE 2 – Trust [ITU-T X.509]: Generally, an entity can be said to "trust" a second entity when it (the first entity) assumes that the second entity will behave exactly as the first entity expects. The key role of trust is to describe the relationship between an authenticating entity and an authority; an entity shall be certain that it can trust the authority to create only valid and reliable certificates.

ITU-Def

- NOTE 3 – Trust [ITU-T X.1163]: The relationship between two entities where each one is certain that the other will behave exactly as it expects.
- NOTE 4 – Trust [ITU-T X.1252]: The firm belief in the reliability and truth of information or in the ability and disposition of an entity to act appropriately, within a specified context.
- NOTE 5 – Trust [ITU-T Y.2701]: Entity X is said to trust entity Y for a set of activities if and only if entity X relies upon entity Y behaving in a particular way with respect to the activities.
- NOTE 6 – Trust [ITU-T Y.2720]: A measure of reliance on the character, ability, strength, or truth of someone or something.

TRUST

Attributes

Social Domain

Confidence	Dependence	Goodness
Belief	Ability	Honesty
Expectation	Faith	Integrity
Surety	Reputation	Assurance

Cyber Domain

Correctness	Completeness	Credibility
Relevance	Accuracy	Confidentiality

Physical Domain

Stability	Dependability	Reliability
Scalability	Reconfigurability	Availability

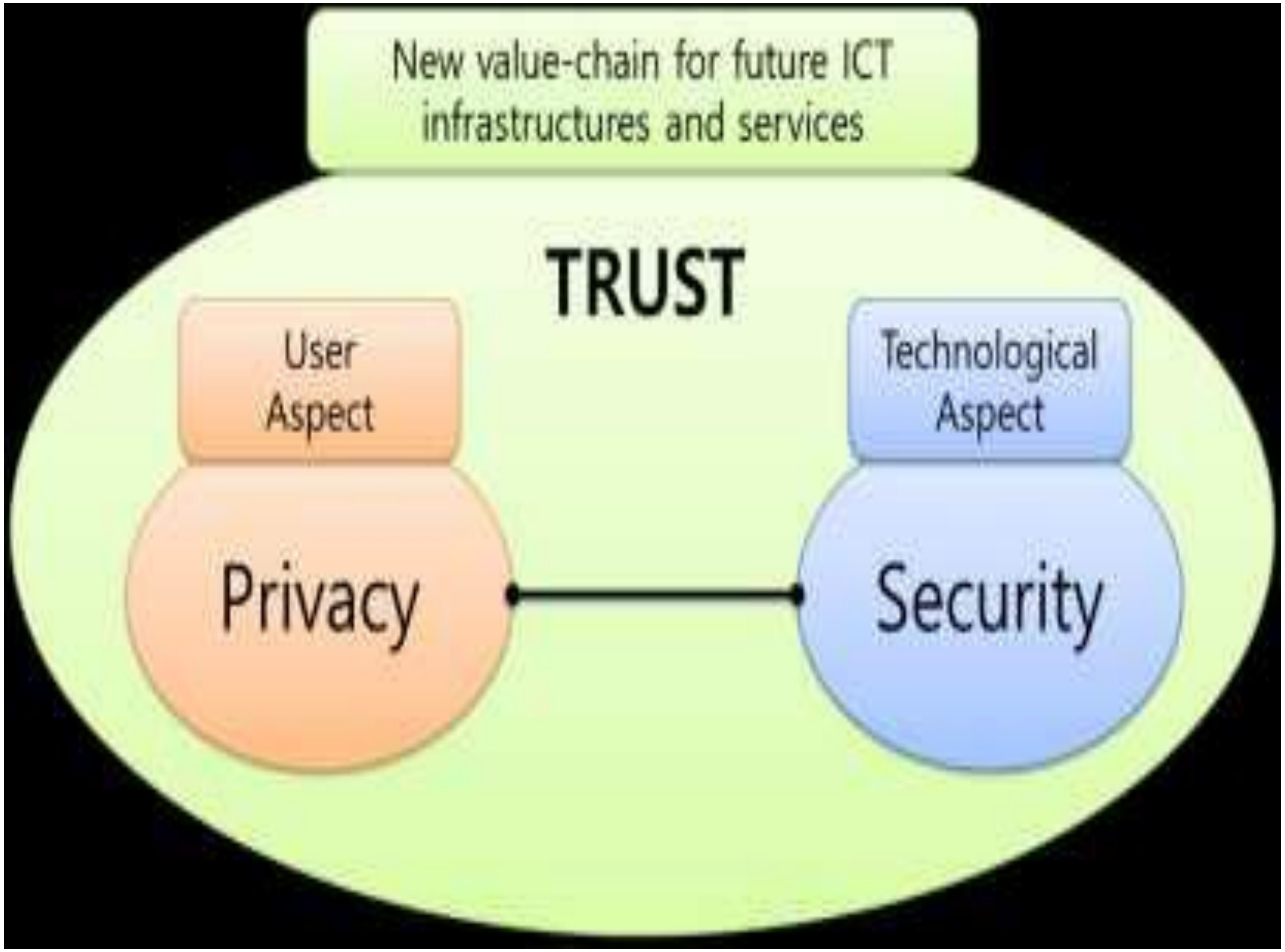
Relationship among security, privacy and trust

- **Security: systems need a variety of methods to prevent behaviours with malicious intents. Security mainly concerns technological aspects such as the confidentiality, availability and integrity. It also includes attack detection and recovery/resilience.**

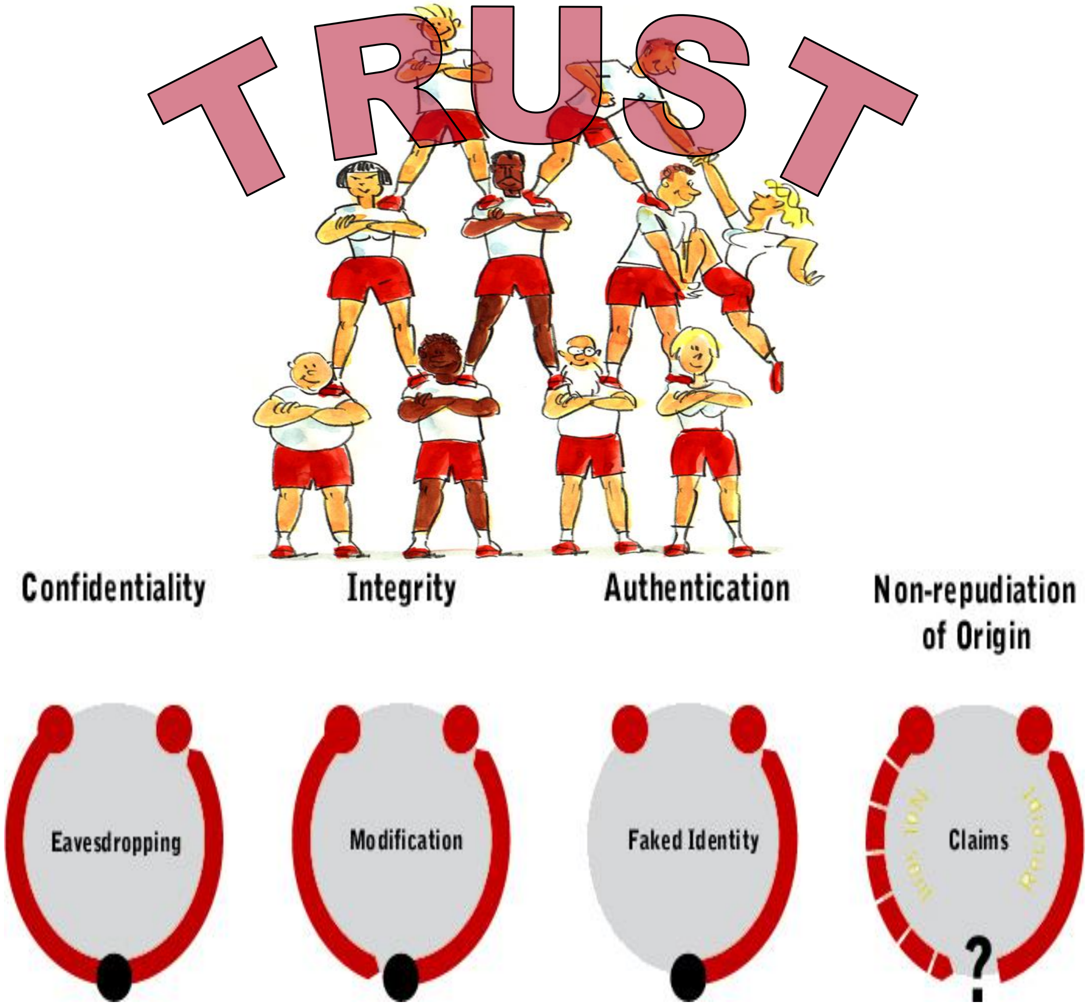
Relationship among security, privacy and trust

- **Privacy: users need the protection of their personal information related to their behaviours and interactions with other people, services and devices. Privacy mainly concerns user aspects to support anonymity and restrictive handling of personal user data.**

Relationship among security, privacy and trust



IoT Needs Trust



IOT- Security –NUTSHELL- Importance

A. Scale of IOT - 2015: 15Bn > 2020: 31Bn > 2025: 75Bn > 2030: 125 Bn (Gartner)

B. Security in IOT comprises of

1.End Point Devices Security
2. Network Communication Security
3. Application Level Security
4. Service Layer Security

Implementing above four security basically leads to Trusted Environment wherein the end user trusts the IOT Ecosystem.

1. Trust in ICT Environments
2. Physical Domain trust
3. Cyber trust
4. Cross-domain service trust

C. IOT - Security >> data / Information Security

Maintain

1. Confidentiality – of data / Information
2. Integrity - " "
3. Availability - " "
4. Accountability - " "
5. Audit ability - " "

•

IOT- Security –NUTSHELL- Importance

D. Some IOT Standards

1. Industrial Internet Consortium (IIC) - : Industrial Internet of Things, Volume G4: Security Framework
2. IEEE Internet of Things – IEEE P-1363, P – 1619, P-2600, P-2413, 802.1AE, 802.1X
3. International Electrotechnical Commission (IEC) - IEC/TR 62443-2-3. “Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment.
4. International Organization for Standardization (ISO) - — Internet of Things Reference Architecture (IoT RA)
5. Cloud Security Alliance -
6. Internet Engineering Task Force (IETF) –
7. ITU-T SG20
8. 3rd Generation Partnership Project (3GPP):
9. oneM2M etc

ISO 9001:2008

- IOT – Security Works at TEC

Release of TR on IOT/M2M security – Works at TEC

- Technical Report on Recommendations in IOT / M2M Security prepared by TEC was Released this year by H'able MoC.
- This was widely circulated to various other Ministries / organisations like MoUd, MoRT,BIS,TSDSI, CDOT, Niti Aayog, ETSI, etc.
- This TR has also invoked interest at NITI Aayog regarding Report and Formation / Finalisation of Framework for NTC.

M-KYC, EPD ,NTC, Use cases

- The Report introduced certain new concepts like:
- Machine – KYC / KYM
- End Point Device Classification
- Classification of Security Requirements as per Use Cases
- Framework for National Trust Centre / Global TC

Define Security for IoT as:

ISO 9001:2008

“ IoT security deals with safeguarding connected devices, physical and virtual, in addition to the networks and IT security, for the Internet of things “

“Whether the support of security services is addressed at the M2M Service Layer level or at the M2M Application level, the ability to establish security associations between corresponding M2M nodes is required. Ideally, this ability could apply to nodes affiliated with different M2M Application Service Providers and M2M Service Providers..”

Issues addressed in TR on Recommendations in IOT/M2M Security

- Incorporation of minimal security standards for M2M products and services with interoperability in view
- Define guidelines from security angle in relation to
  - **Data ownership and retention period**
  - **Security of sensitive data (privacy and security concerns)**
  - **Location of application services**
  - **Location of remote terminal unit/M2M devices**
  - **Location of core network elements**
- Enable interconnection of legacy/non-IP devices on existing network technologies
- Define precautions/security conditions for voice/SMS/MMS/video on M2M
- Security framework for various verticals and solutions
- KYC norms for M2M, Concept of Machine - KYC
- M2M Product Certification **(as per TEC MTCTE Scheme, Launched in July 2019)**
- The End User and Industrial User of the new M2M / IoT Applications, whose safety, ease-of-use and interests must be safe-guarded
- The Government Policy makers must act in the interest of the enablement of Industry

IOT-Security

- The future of IoT/M2M cannot be realized without addressing security and privacy risks and policy issues.
- Securing and protecting the things that matter most—our systems, our Data, and our privacy—is a shared responsibility.
- Security and privacy must become part of every product's feature set.

IOT-Security: Affected Stakeholders

- The Following stakeholders are affected by the IoT/M2M Security threats
- M2M Application Service Provider;
- Manufacturer of M2M Devices and/or M2M Gateways;
- M2M Device/Gateway Management entities;
- M2M Service Provider;
- Network Operator
- User/Consumer

IoT Functional Architecture

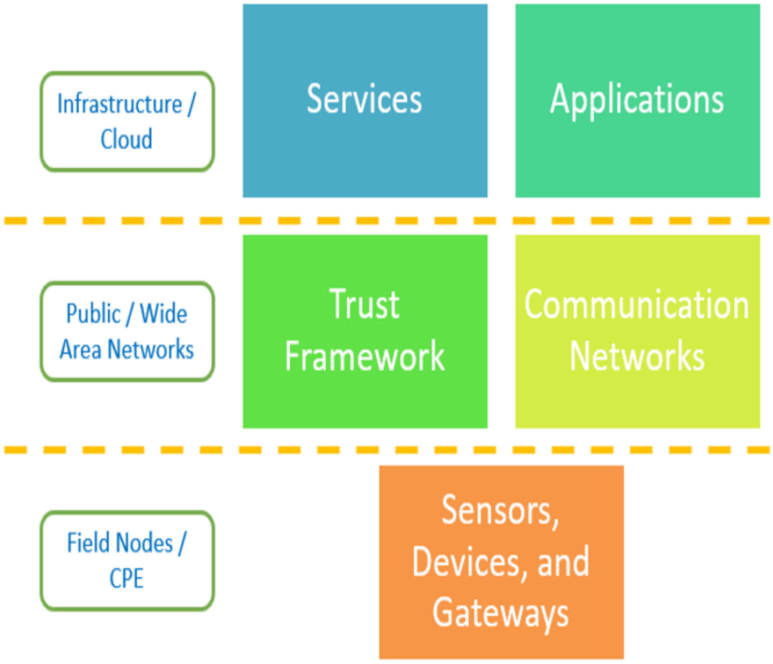


Figure 5: Functional View

- IoT Architecture can be understood in 5 blocks
  - Sensors, Devices and Field Nodes
  - Communication Networks
  - Trust Frameworks
  - Applications
  - Common Services Layer

End Point Device security

- Do all End Point Devices need to confirm to same level of Security ?
- One must arrive at a logical and practical solution, as EPD security will entail costs and consume other scarce resources like memory, power etc.
- Hence the various Assuarance classification level proposed.

End Point Device security

- End Point Devices:The End Point Devices form the most essential part of the machine to machine network, as it is here that the data creation / information generation / actuation happens.The most significant aspect of security for End Point Devices is to establish the assurance level of End Point devices, as they manifest themselves in different forms with unique requirements of the use cases they serve.
- The graphical representation in the section below defines the requirement and the alternate security levels which may be used as per customer requirement and the specific security needs of the use case.
- The security as well as the authentication infrastructure should be defined based on the required assurance level and the need for security in the use case.

Reducing Risks in IoT/M2M Solutions: End Point Devices

ISO 9001:2008

End Point Devices:

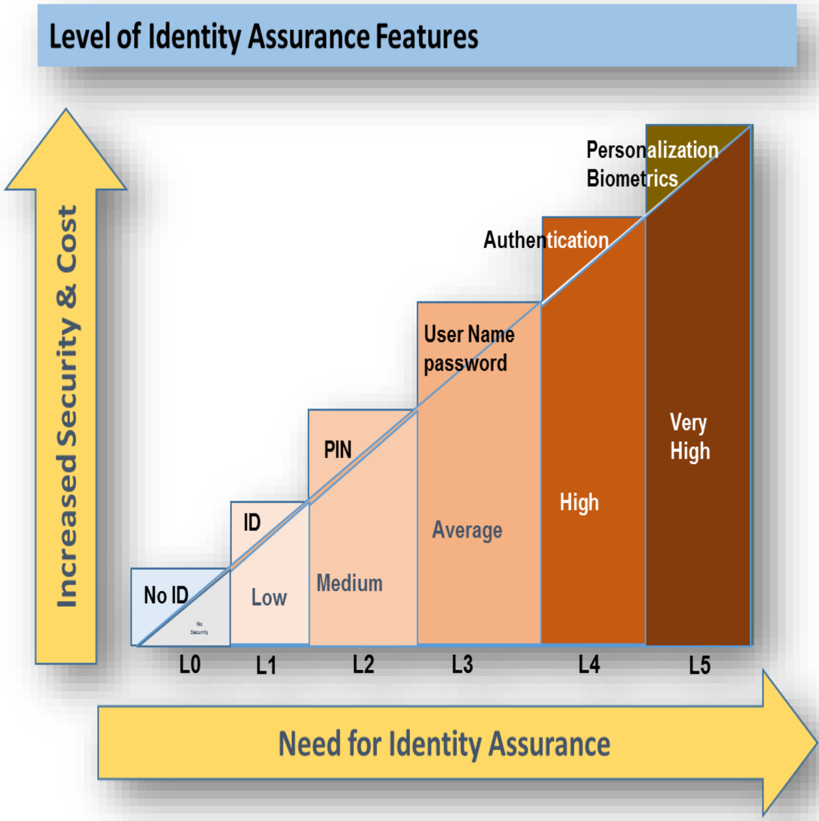
The End Point Devices form the most essential part of the machine to machine network, as it is here that the data creation / information generation / actuation happens.

Security by Design is critical

Establishment of assurance level of End Point devices based on use case classification is key

End to End Security must start from provision of secure keys at the end point devices

UICC as a Secure Token for 3GPP / multi technology access Devices



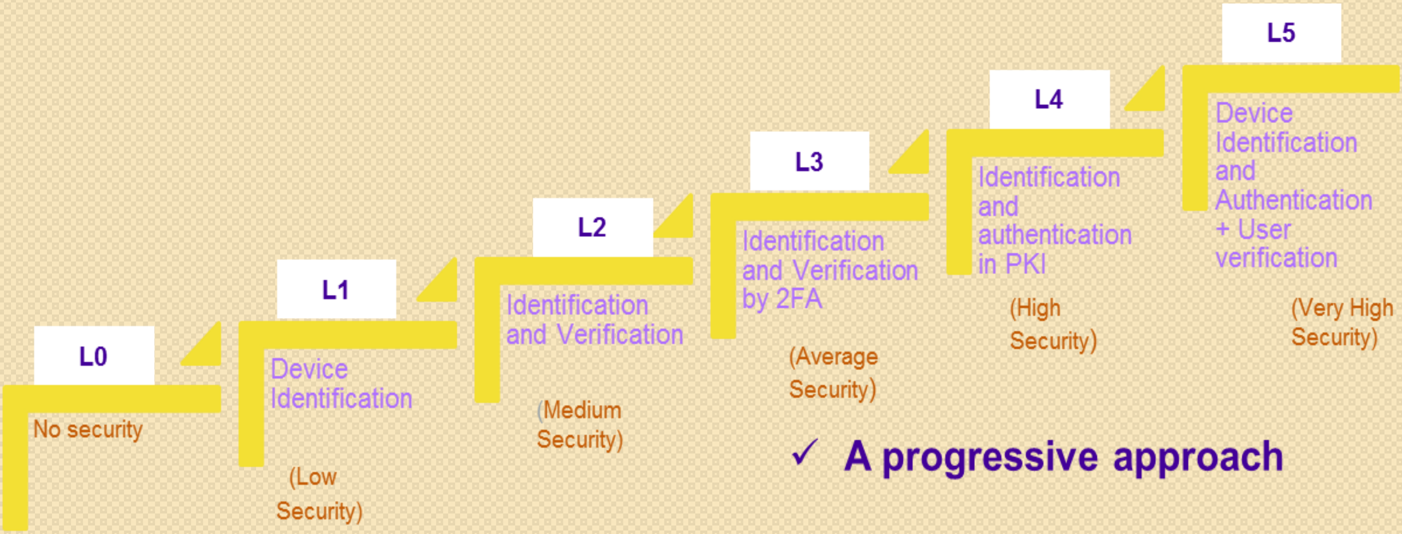
Level of Identity Assurance Features

Increased Security & Cost

Need for Identity Assurance

L0	L1	L2	L3	L4	L5
No ID	ID	PIN	User Name password	Authentication	Personalization Biometrics
No Security	Low	Medium	Average	High	Very High

Assurance Level For EPD as per security Requirements



L0

No security

L1

Device Identification

(Low Security)

L2

Identification and Verification

(Medium Security)

L3

Identification and Verification by 2FA

(Average Security)

L4

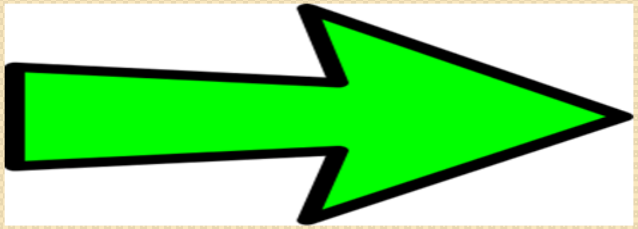
Identification and authentication in PKI

(High Security)

L5

Device Identification and Authentication + User verification

(Very High Security)



- ✓ **A progressive approach**
- ✓ **Simple to complex level**
- ✓ **Different segment different need**
- ✓ **Scalable and Commercial viable**

Network Communication security-IOT

- It is imperative that the protocol stack of an M2M device has a robust and well protected Management and Control frames to prevent access to the information stored in the devices which can be used by an attacker to compromise not only the device but the entire M2M eco-system.
- Each entity in the M2M services chain should be responsible for the KYC of its customer, i.e. bulk KYC for the B2B relationships and the final customer facing entity, i.e. the B2C, should be responsible for fulfilling the customer's KYC requirements.
- Just as an owner of the SIM is responsible for informing the TSPs for effecting any change in ownership of the SIM, similarly, the first / existing owner of the device (especially white goods, medical devices, cars, etc) should be responsible for transfer of ownership, in case the device changes hands. This would take care of the concerns of the security agencies about the traceability of the user of the end device.
- e-KYC should be mandatory for KYC by the MSPs

Application Level Security

- In the Machine to Machine domain, critical components of Application logic are implemented and distributed in a number of End Points, Gateways and Servers. Most current prevalent distributed computing software development models use the client side to initiate server requests and a remote server side to process these requests (the client-server model). This allows application developers to take advantage of centralized security, compute and storage and that has been a major driver of the emergence of cloud computing.

Application Level Security

- However, for M2M applications, developers need to identify features of their applications that require processing at the edge as distinct from features that require high compute power or that do not require near real-time response and can, therefore, be deployed at a central location. Each application service logic can be resident in a number of End Points and/or more than once on a single End Point (EP). The EP can be a traditional Smartphone or other wireless connected compute elements in a car, smart home or industrial location that can run dedicated client applications

Application Level Security

- Each execution instance of an application service logic may be termed an “End Point Application Instance (EPAI)" and is identified with a unique Identity. Examples of the EPAIs include an instance of a fleet tracking application, a remote blood sugar monitoring application, a power metering application, or a controlling application.

Application Level Security

- Though End Points are assumed to communicate without human involvement, individuals or organizations remain responsible for setting the access control policies used to authorize their EPAIs to access M2M Application services. In particular, individuals or organizations acquiring the End Points can subscribe to a contract with an M2M Service provider (M2M Service Subscription) under which they enrol their End Points (e.g. using identifiers pre-provisioned on the End Points, such as End Point-ID).

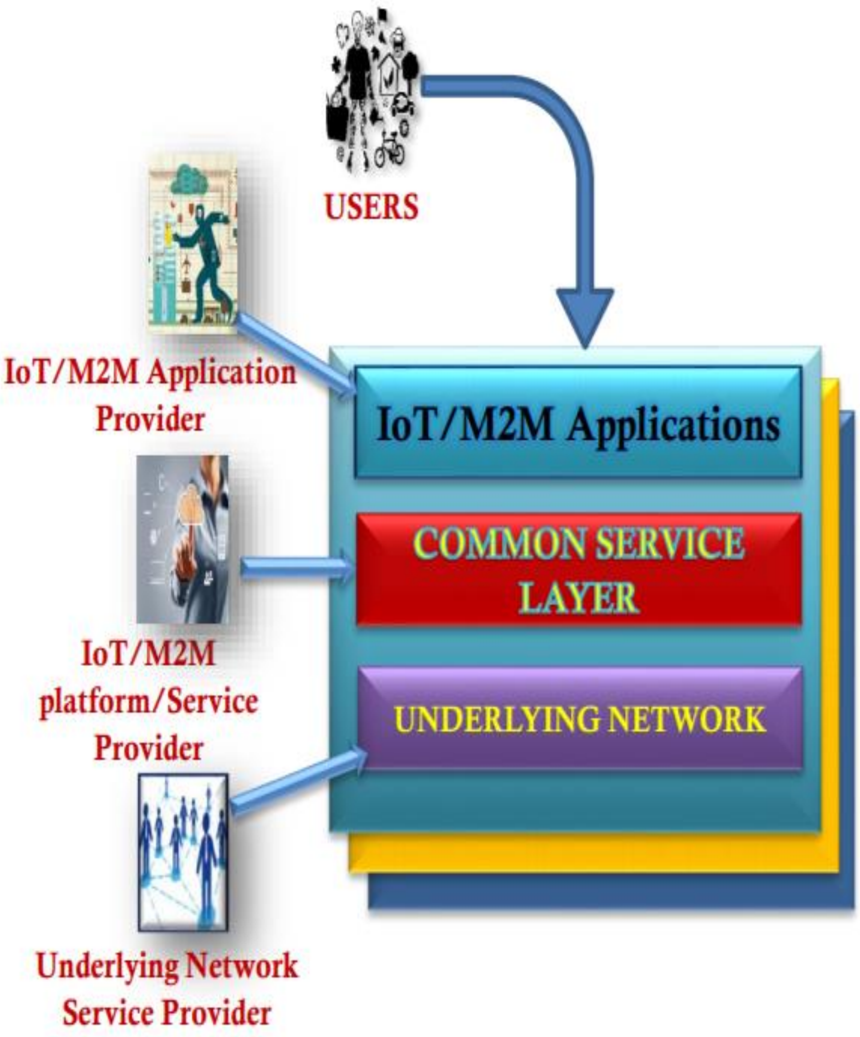
Application Level Security

- This in turn may require an M2M Service provisioning step (including Security provisioning) that takes place on the target End Points themselves, for which interoperable procedures are specified by Standards. Following the M2M service provisioning, the End Points can be identified and authenticated by an M2M Authentication Function for association with an M2M Service Subscription, whose properties reflect the contractual agreement established between their owner and the M2M Service Provider.

Application Level Security

- Similarly, it must be necessary for the M2M Service Provider to ensure that the EPAIs accessing M2M services be provisioned with security credentials that are used to authorize specific operations to instantiated applications. This step is required to manage the deployment and management of applications that are instantiated in great numbers, as it enables all instances of an application to be managed through common security policies that are set once for all.

Roles in an IoT Ecosystem


USERS
IoT/M2M Application Provider
IoT/M2M platform/Service Provider
Underlying Network Service Provider
IoT/M2M Applications
COMMON SERVICE LAYER
UNDERLYING NETWORK

Functional Role Description

1. The *User* (individual or company) fulfils all of the following criteria:
   a. Uses an M2M solution.
2. The *Application Service Provider* fulfils all of the following criteria:
   a. Provides an M2M Application Service.
   b. Operates M2M Applications.
3. The *M2M Service Provider* fulfils all of the following criteria:
   a. Provides M2M Services to Application Service Providers.
   b. Operates M2M Common Services.
4. The *Network Service Provider* fulfils all of the following criteria:
   a. Provides Connectivity and related services for M2M Service Providers.
   b. Operates an Underlying Network. Such an Underlying Network could e.g. be a telecom network.

Security Classification Framework

Security Classification

- Registration of M2M SP and M2M ASP
- Classification of IoT / M2M Applications / Use Cases
- Specifications, Certification and Compliance for IoT / M2M Devices by **Use Case Categories**

Security Classification Framework

- Registration of M2M SP by a Competent Authority recommended by DoT
- Registration of M2M ASP by Registrars within the Industry Vertical [ARAI, IMA, MEITY, ISGF etc] but preferably a single national registrar, the National Trust Centre
- Connected Device / Gateway Manufacturer Certification (e.g. TEC MTCTE Launched in July 2019)
- A National Registrar for all M2M Machines, Embedded Tamper resistant Identity that can enable a Machine KYC
- Specifications, Certification and Compliance for IoT / M2M Devices by Use Case Categories
- Identity, Version and Configuration details registered along with the Machine KYC holder

Concept of Machine – KYC / KYM

- The present licensing and regulatory regime is totally focused on provisioning of Voice and Data service for usage by humans. Accordingly, it covers issues such as customer acquisition, their KYC, customer data retention and sharing, security and LEA requirements, QoS compliances, tariff controls, roaming, etc. However, M2M services encompass a plethora of other services that have evolved from the IT domain. KYC of any customer is mandated for any individual utilizing human to human communication services. Similarly, it shall be prudent to ensure KYC of the OEMs of the machine(s) / device(s) and that of the ultimate owners of that machine / device

Concept of Machine - KYC

- The concept of "Machine KYC" is fast becoming relevant, especially in the backdrop of remote connected dispersed and mobile assets such as Vehicles, Meters etc. It is not sufficient to know the identity of the owner (person) of the connectivity element, but equally important to know the Machine in which the connectivity element is fitted in. The National Trust Centre will identify "Machines" based on tamper resistant connectivity elements, which will add to the security, safety and traceability of the IoT use cases

Concept of Machine - KYC

- The current guidelines listed for adherence to KYC norms, for the telecom services, are onerous and impractical to implement while provisioning M2M services as the devices / automobiles are movable assets and often change hands. Purchase and sale of movable assets decisions are individual centric and it shall be extremely difficult and economically unviable for the MSP/TSP to keep track of the chain of events post sale and resale of devices/automobiles. Therefore, a simpler solution shall have to be evolved for implementing KYC norms for the M2M devices. Following suggestions are made towards this end

Concept of Machine - KYC

- Suggestion
- The KYC norms for each of the individual M2M service verticals should be part of the TEC standards finalization agenda.
- For the automobiles, the MDN can be captured as part of the registration process, similar to the engine and chassis numbers. The activation / deactivation of the SIM should be permitted only once the copy of RC is submitted to the TSP by the original / subsequent purchaser. (suggestion)

Concept of Machine - KYC

- suggestion
- For devices which are owned by an individual, e.g. white goods / health products, the ownership of MDN can be with the customer (purchaser) itself. The original / second / subsequent purchaser shall approach his local TSP for the MDN, of the M2M device, and hence his KYC details can be captured as per the existing norms. This would also provide the customer the flexibility of (a) subscribing / not for the M2M services, (b) choosing the network provider of his choice depending on the coverage in his area as well as (c) ensuring that he retains the number of his choice while subscribing to M2M services

Concept of Machine - KYC

- M2M KYC has to be implemented as a security by design. Machine KYC implies that the device is an authenticated device [e.g. a Certified Device and / or a registered Vehicle/Machine from an OEM/OE registered in India] installed with a tamper resistant identity [e.g. a secure element] in a manner that any removal / replacement of the Secure Element / Device from the Vehicle / Machine in which the Secure Element / Device is installed should immediately raise an alarm through the secure element and the device application, rendering the device unusable with the other Vehicle / Machine, unless explicitly authorised by the registered M2M Service Provider providing the Service. The concept may be implemented through the following steps:

Classification of Use Cases

- The most important aspect of M2M / IoT Security is in how it is able to protect the data generated by the end points and the applications that use the end point data to create services. The classifications of IoT / M2M Use Cases, and the proposed mandatory recommendations, are in the context of the said primary objective of M2M / IoT data protection
  - Use Case categories
    - **Mission Critical, High QoS, Sensitive Information [CQS]**
    - **Mission Critical, High QoS, Non Sensitive Information [CQN]**
    - **Non Critical, Best Effort, Sensitive Information [NBS]**
    - **Non Critical, Best Effort, Non Sensitive Information [NBN]**
    - **Mission Critical, Best Effort, Sensitive Information [CBS]**
    - **Mission Critical, Best Effort, Non Sensitive Information [CBN]**
    - **Non Critical, High QoS, Sensitive Information [NQS]**
    - **Non Critical, High QoS, Non Sensitive Information [NQN]**

Trust Model

Registration for IoT / M2M domain

- Recommendations : all IoT / M2M Service Providers and IoT / M2M Application Service Providers shall be registered with the Department of Telecommunications as per the draft M2M Service Providers (M2MSP) Registration Guidelines
- M2MSP / M2MASP be given a unique identity with a Company Name, Registration_ID, Application_Name, Application_ID, Application_Classification, Start_Date , (PPS of Company)
- Hosting of the M2M Service Provider Applications shall be from Cloud or Privately Hosted Servers physically located in India
- IP address(es) used by the M2M Service Provider shall belong to a range of valid IP addresses from Indian Registry for Internet Names and Numbers, issued by a licensed ISP / Domain Name provider in India
- Exactly one Server Node per Infrastructure Domain per M2M Service Provider

- Common Service Functions
  - Security Common Services Function hosted by the M2M Service Provider shall ensure implementation of the security functions described below
    - Record the Embedded Machine Identity or "Machine KYC"
    - Identify the Machine's Capability, Configuration and Purpose or Use Case
    - Record the Identity [APP ID] of the Application / Server that the Machine is parented to
    - Record the Identity [M2M SP ID] of the M2M Service Provider who is responsible for the Machine with the possibility of admitting changes of the M2M SP
    - Identify the Owner of the Machine with the possibility of admitting changes of the owner
    - Command the Machine to reveal its Identity, configuration
    - Ensure Location Discovery
    - Locking of the Connectivity element to the Remote / Dispersed / Mobile Object
    - Ensure Lawful Intercept and Block / Shut Down
  - Remote Provision able Connectivity
  - High Quality of Service in Connectivity meant for mission critical use cases

National Trust Centre

- National Trust Centre

A National Trust Centre be formed under the Umbrella of DoT to implement .

- Recommended Framework for National Trust Centre
  - Registration of M2M Service Providers
  - Registration of M2M Applications using a Class 2 / Class 3 Certificate taken from the Commercial CA in India
  - M2M ASP interactions coupled through standards based m2m architectures
  - Registration of Devices, which may include following
    - Record the Embedded Machine Identity or "Machine KYC"
    - Identify the Machine's Capability, Configuration and Purpose or Use Case
    - Record the Identity [APP ID] of the Application / Server that the Machine is parented to
    - Record the Identity [M2M SP ID] of the M2M Service Provider who is responsible for the Machine with the possibility of admitting changes of the M2M SP
    - Identify the Owner of the Machine with the possibility of admitting changes of the owner
    - Command the Machine to reveal its Identity, configuration
    - Ensure Location Discovery
    - Locking of the Connectivity element to the Remote / Dispersed / Mobile Object
    - Ensure Lawful Intercept and Block / Shut Down
  - Remote Provision able Connectivity
  - High Quality of Service in Connectivity meant for mission critical use cases

Common Mandatory Security Requirements

Node	Mandatory Parameter	Specification / Requirement / Standard
Device	Identity	As per ANSI 41 / ITU
	Certification	TEC Certified
	SIM Locking to IMEI	Required for Pluggable Form Factor
	Application Authorization	Required
	Device Data	End to End Encryption
	Remote Management	Real time Request / Response for Identity & Configuration
Application	IoT / M2M Service Provider ID	DoT Provided
	IoT / M2M Application ID	National Trust Centre Provided
	IoT / M2M Server ID	As per IoT / M2M Service Provider Registration
	Practice Statement	Required, Published, Updated

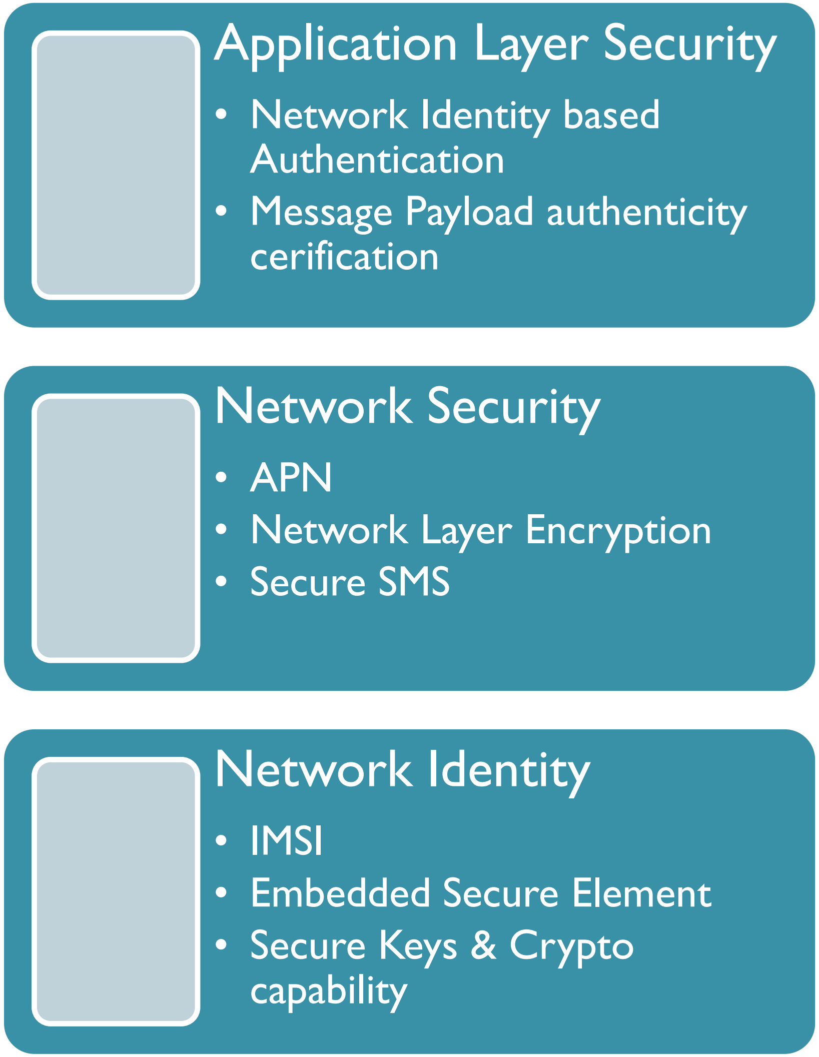
Use Case Class Specific Mandatory Security Requirements

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		*	

Reducing Risks in IoT/M2M Solutions | Network Layer

Network Layer

- Network Layer is critical to implementing end to end security, it natively offers a tamper resistant security infrastructure
- Each entity in the M2M services chain should be responsible for the KYC of its customer, e-KYC should be mandatory for KYC by the M2M Service Provider (M2M SP)
- SIMs should be issued with Indian IMSIs India, where they are embedded in devices sourced abroad, they must be converted to Indian IMSIs by Over-The-Air (OTA) Provisioning within an year / six months.
- M2M SIMs, being industrial grade and embedded, are costlier than the normal SIMs and require a completely different business model and lifecycle management. The M2M SIMs should be permitted to be procured by the MSPs, SIM Ownership with MSPs
- MCC and MNC should not be directly allocated to the MSPs
- India needs to negotiate maximum number of MLAT agreements
- M2M SIMs should be issued with restrictive guidelines, M2M SIM management infrastructure should be based in India
- Generic Bootstrapping for Access Control



Application Layer Security

- Network Identity based Authentication
- Message Payload authenticity cerification

Network Security

- APN
- Network Layer Encryption
- Secure SMS

Network Identity

- IMSI
- Embedded Secure Element
- Secure Keys & Crypto capability

Reducing Risks in IoT/M2M Solutions | Application Layer

Application Layer

- In the M2M domain, critical components of Application logic are implemented and distributed in a number of End Points (EPs), Gateways and Servers
- Registration and Identification of the M2M Service Provider (M2M SP) and M2M Application Service Provider (M2MASP) and Application Layer Instances by a Registration Authority
- The Registration Authority may be a National Trust Centre that can Identify Certified M2M Applications and Devices
- The Platform Layer must implement an authentication function for identifying and authorising EPs, validate the credentials provided to the EPs during the M2M application enrolment procedures

Strong Authentication & Security

- A minimum use of Private or Public Keys, 3DES / AES / AKA algorithms
- Identification and Encryption of Sensitive and PII data, Secure storage of Sensitive Application Data
- Mechanisms for generating Application Layer alerts when QoS, Safety, Security and Reliability conditions are compromised
- Health Packets, Heartbeat mechanisms between End Points and Apps
- Fraud detection, FMEA and Analytics in order to minimise breakdowns

Reducing Risks in IoT/M2M Solutions | Application Layer

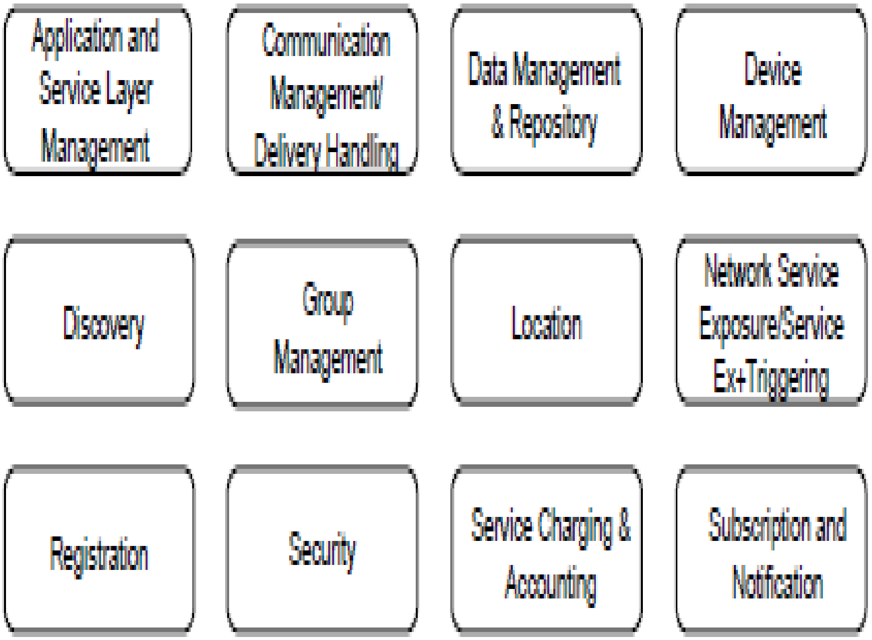
ISO 9001:2008

- Establishment of a Secure Association by generating a security credential (M2M Connection key), which must be shared between communicating End Points / App Layer
- Resistant to Man-in-the-Middle Attacks, Replays, DDOS
- Remote and Secure updates of security parameters in EP Firmware
- Locking of the tamper resistant Secure Element with Device / Asset Identity
- Blocking of Services until E-KYC and registration is completed, or if compromised
- Compliance to DoT / MIETY Guidelines for storage of Data in India, Identification of the IPs / Location of Application Servers, Platforms and Network Elements, Lawful Interception
- Minimum Data Retention and Archival as per Standards and Guidelines
- Management of Sensitive functions executing operations on sensitive data
- Secure Device Management to ensure protection of EP configuration, such as destination IPs, Frequency of Data

Reducing Risks in IoT/M2M Solutions | Common Service layer

Common Service Layer

- Most M2M solutions in different industries use proprietary systems that often comprise all layers, from physical to application, to provide their specialized M2M services to customers
- There is a need for a standardized common service layer that can enforce common security principles, data sharing, inter-operability, transferability and device management
- The Common Service Layer sits between the Applications and the underlying Communication Layer
- It exposes common set of functions to applications via developer friendly APIs
- It is integrated into devices/gateways/servers and allows distributed intelligence
- It hides complexity of NW usage from apps, stores and shares data, supports access control, notifies applications about events
- By deploying the Standards compliant Common Service Layer, M2M Service Providers can offer wide range of services developed by the industry

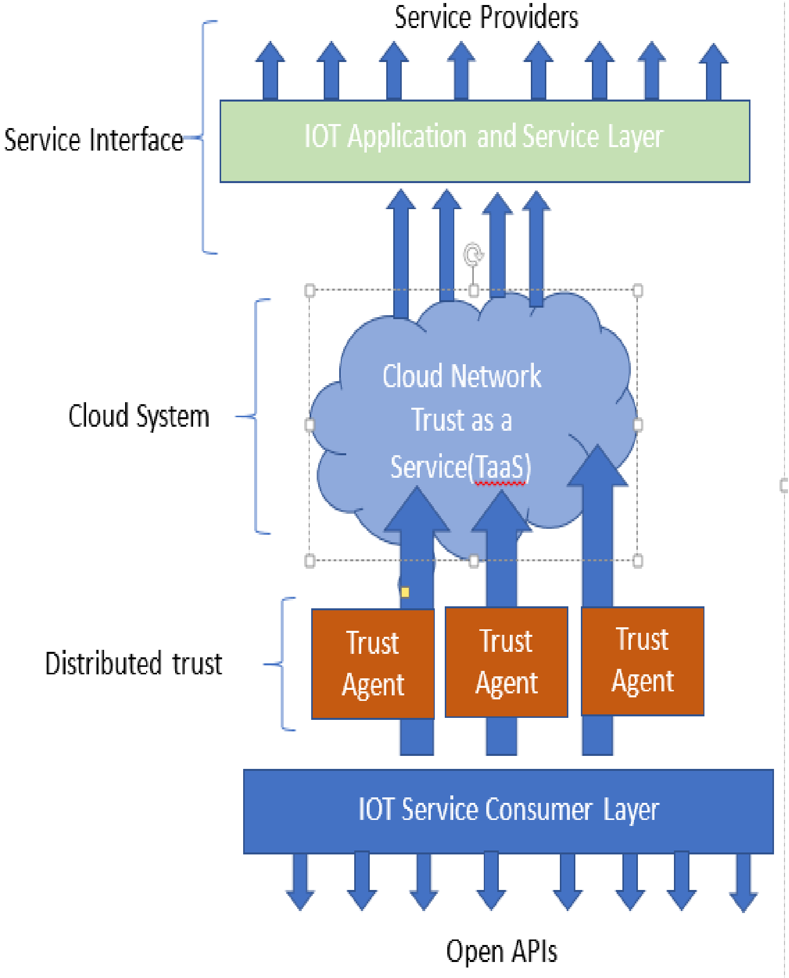


Application and Service Layer Management	Communication Management/ Delivery Handling	Data Management & Repository	Device Management
Discovery	Group Management	Location	Network Service Exposure/Service Ex+Triggering
Registration	Security	Service Charging & Accounting	Subscription and Notification

Reducing Risks in IoT/M2M Solutions | Trust Framework

Trust Framework

- National Trust Centre for M2M Devices and Applications should be mandated
- Trust means that an entity behaves in a particular defined way. A trusted resource is one that is forced by its constitution to function in a trusted manner.
- The failure of this resource would compromise the function, integrity or security of a system which does not give output / result in expected ways
- The trusted ICT infrastructure comprise objects from the physical domain (physical objects), the cyber domain (virtual objects) and the social domain (humans with attached devices), which are capable of being identified and integrated into information and communication networks
- Employ Identity management with digital identification/authentication of social-cyber-physical objects.
- SIMs should be issued with Indian IMSIs India, where they are embedded in devices sourced abroad, they must be converted to Indian IMSIs by Over-The-Air (OTA) Provisioning within an year / six months.
- Maintenance and periodic analytics of Trust Data including operations of objects and the history of interactions
- Trust model must enable cross-domain and cross-certification trust model



TEC-Works Contd

- A contribution on M-KYC has been prepared to be submitted to ITU and is under discussion and finalisation in NWG 17
- Similarly a Contribution on EPD classification and Requirements of Security as per Use Cases are under preparation to be submitted to ITU
- Framework for NTC is being worked out by Sub-Groups LPCC's and is under Finalisation as interest of Niti Aayog for its Implementation

TEC-Works Contd

- For Dissemination of Information Tec has conducted various Webnairs
- Webnair on " App Id Registry " 0n 3rd July 2019 by LPCC Sh Sharad Arora, Ms Sensorise
- Webnair on " IOT Security " also covering NTC Framework on 17th July 2019 by DDG SN under the aegis of India EU ICT Project.
- Deliberations are going on for Finalisation of NTC Framework amongst various Subgroups for Conclusion.

ISO 9001:2008

- TEC has now been granted ISO 901:2015 Certification
- An Ardent , inquisitive reader can always access the TR on IOT / M2M Security from TEC website under M2M / IOT Reports and feedback from all are welcome for improvement and next version of the report, on mail: dirsn.tec@gov.in, adgsn-dot.tec@gov.in, ddgsn.dl.tec@gov.in,

ISO 9001:2008

THANK YOU

From

SN Division TEC,

New Delhi, India.

07-09-2018

Website: www.tec.gov.in