सत्यमेव जयते

TECHNICAL REPORT

Framework of

National Trust Centre for

M2M/ IoT Devices and Applications

TEC 31188:2022

WORKING GROUP: Security by Design and National Trust Centre

ISO 9001 :2015

TELECOMMUNICATION ENGINEERING CENTRE
DEPARTMENT OF TELECOMMUNICATIONS
MINISTRY OF COMMUNICATIONS
GOVERNMENT OF INDIA

RELEASE 1.0

MARCH, 2022

Revision History

Date	Release	Document No.	Description
March, 2022	R1.0	TEC 31188:2022	Framework of Nataional Trust Centre for M2M/IoT Devices and Applications

Important Notice

Individual copies of the present document can be downloaded from TEC website using link **(https://www.tec.gov.in/M2M-IoT-technical-reports)**

Users of the present document should be aware that the document may be subject to revision or change of status.

Any comment/suggestions may please be sent to: **m2mreports.tec@gov.in**

Disclaimer

The information contained is mostly compiled from different sources and no claim is being made for being original. Every care has been taken to provide the correct and up to date information along with references thereof. However, neither TEC nor the authors shall be liable for any loss or damage whatsoever, including incidental or consequential loss or damage, arising out of, or in connection with any use of or reliance on the information in this document. In case of any doubt or query, readers are requested to refer to the detailed relevant documents.

Table of Contents

List of Contributors

A. Joint Working Group (JWG) Chairman:

Name	Designation	Organisation	E-mail Address
Ms. Deepa Tyagi	Sr. DDG & Head TEC	Telecommunication Engineering Centre (TEC)	srddg.tec@gov.in

B. List of chairs

Designation	Name	Organization	e-mail address
Chairman	Sushil Kumar	TEC	ddgsd.tec@gov.in
Vice Chairman	Sh. Aurindam Bhattacharya	CDOT	aurindam@cdot.in
Rapporteur	Sh. Prashant Pandey	M/s STMicroelectronics Ltd.	prashant-mpa.pandey@st.com
Co- Rapporteur	Ms. Ashima	TEC	dirsd1.tec@gov.in
Co- Rapporteur cum Convenor	Sh. Shekhar Singh	TEC	ad.iot-tec@gov.in

C. List of contributors

S. No.	Name	Organization	e-mail address
1.	Sushil Kumar	TEC	ddgsd.tec@gov.in
2.	Sh. Aurindam Bhattacharya	CDOT	aurindam@cdot.in
3.	Sh. Prashant Pandey	M/s STMicroelectronics Ltd.	prashant-mpa.pandey@st.com
4	Sh. Pranav Singh	IDEMIA	pranav.singh2@idemia.com
5	Ms. Ashima	TEC	dirsd1.tec@gov.in
6	Sh. Amit Rao	M/s Trusted Objects	a.rao@trusted-objects.com
7.	Sh. Arvind Tiwary	IoT Forum	arvind_t@sangennovate.com
8.	Sh. Sharad Arora	M/s Sensorise Technologies Pvt. Ltd.	sharad.arora@sensorise.net
9.	Sh. Shekhar Singh	TEC	ad.iot-tec@gov.in
11.	Sh. Raunaque Mujeeb Quaiser	M/s STMicroelectronics Ltd.	Raunaque.quaiser@st.com

S. No.	Name	Organization	e-mail address
12.	Sh. Narang kishore	M/s Narnix Technolabs Pvt. Ltd.	kishor@narnix.com
13.	Sh. Dinesh Sharma	SESEI (ETSI)	dinesh.chand.sharma@sesei.eu
14.	Sh. Nitin Sharma	SESEI (ETSI)	nitin.sharma@sesei.eu
15.	Sh. Vijay Madan	TSDSI	vijay.madan@tsdsi.in
16.	Sh. Rajendra Saini	M/s DELL Ltd.	rajender.saini@dell.com
17.	Sh. Vinosh Babu James	M/s Qualcomm	vinosh@qti.qualcomm.com
18.	Dr. R Lenin Raja	M/s Electromagnetic Test Laboratory, Gurgaon	dr.lenin@aaemtlabs.com
19.	Ms. Namrata Singh	TEC	namrata.singh51@gov.in

1. Introduction

IoT / M2M technology has been in use in the industrial domain for many years where sensors and automated manufacturing processes have made the industrial sector efficient. As, the use of those devices and applications were limited to the premises of the respective industries, the need for securing such devices and applications were not so crucial. However, for the past few years IoT/M2M technologies have started shaping the way of life for citizens across the globe. Today, IoT/M2M technology is being used to create smart infrastructure in various verticals such as Power, Automotive, Safety & Surveillance, Health care, Agriculture, Smart homes and Smart cities etc.

Therefore, the security of the elements in the IoT ecosystem ranging from devices to the applications has become paramount as the devices / networks being used in the IoT/M2M ecosystem may be hacked to harm the companies, organisations, nations and most importantly, the people. It may cause total collapse of the services, thereby creating panic and may also result in havoc.

Ensuring end-to-end security for connected IoT devices is key to the success for IoT eco-system, as without security, IoT will cease to exist. Privacy of the data of the individual is very important especially in the health care domain.

According to a new market research report published by Markets and Markets, the global Internet of Things (IoT) Security Market size is expected to grow from USD 12.5 billion in 2020 to USD 36.6 billion by 2025, at CAGR of 23.9 percent during the forecast period[1].

In view of the anticipated growth of IoT devices, it is essential to ensure that the IoT end points comply to the safety and security standards and guidelines in order to protect the users and the networks that interact with these IoT devices. Every telecom equipment must undergo mandatory testing & certification prior to sale, import or use in India, in compliance to the MTCTE[2] (Mandatory Testing and Certification of Telecom Equipment) guidelines issued by Department of Telecommunications (DoT), Government of India under the Indian Telegraph (Amendment) Rules, 2017. Testing is to be carried out for conformance to Essential Requirements (ERs) prepared by TEC. ERs are available on TEC MTCTE Portal[3].

Telecom Regulatory Authority of India (TRAI) in its recommendations on Spectrum, Roaming and QoS related requirements in Machine-to-Machine Communications released in September 2017 has also mentioned the following two work items related to IoT security.

1) *Device manufacturers should be mandated to implement "Security by design" principle in M2M devices manufacturing so that end to end encryption can be achieved.*

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

[1] https://www.marketsandmarkets.com/PressReleases/iot-security.asp
[2] https://tec.gov.in/mandatory-testing-and-certification-of-telecom-equipments-mtcte
[3] https://www.mtcte.tec.gov.in/

These recommendations were accepted by DoT and communicated to TEC with the addition in recommendation no. (2) above as "*However, DoT also decided that for certification of software products & applications related M2M devices, STQC (Standardization Testing and Quality Certification)*[4] *under MeitY (Ministry of Electronics and Information Technology) may be the agency to carry out such testing under single window of proposed National Trust Centre*" to carry forward the work:

To study these work items, TEC formed a multi-stake holder Working group to have detailed discussion and prepare the report based on global standards and international best practices.

Security by design work item mentioned at point number (1) above will help in the development of secured IoT device and the work item at point number (2) is expected to create the trusted IoT devices eco system by means of testing and certification.

Testing and Certification of IoT devices hardware is already covered in Essential Requirements (ERs) under MTCTE having testing specifications related to EMC, Safety, communication interfaces, IP, SAR and Security. Security specifications being prepared in ITSAR (Indian telecom security assurance requirements) are the part of the ERs. Software of the IoT devices will be tested by STQC (some specifications in annexure-III).

Essential requirements (ERs) for testing of IoT devices under MTCTE have already been prepared and available on TEC MTCTE portal.

Chapter 2 covers various challenges and the mitigation. Progress of the work and NTC visualization as well as concept for implementation has been described in Chapter 3.

[4] https://www.stqc.gov.in/software-testing-and-assessment-0

2. Security Challenges and mitigation

2.1. Challenges related to IoT devices

IoT devices, services and software, and the communication channels that connect them, are at risk of attack by a variety of malicious parties, from casual hackers to professional criminals or even state actors. Possible consequences to consumers of such an attack could include:

- Devices on Risk
- Impact on Individuals, community, and risk to the nation
- Inconvenience and irritation
- Infringement of privacy
- Loss of life, money, time, property, health, relationships, etc.

For vendors, operators, suppliers and integrators, potential consequences may include loss of trust, damage to reputation, compromised intellectual property, financial loss and possible prosecution.

Malicious intent commonly takes advantage of poor design and unsecure software assets. Even unintentional leakage of data due to ineffective security controls can bring dire consequences to consumers and vendors. Thus, it is vital that IoT devices (Cellular and LPWAN) and services have security designed in from the outset. Exponentially growing IoT ecosystem is moving towards industry 4.0 by employing automation, machine learning and real-time data. There will be security challenges, due to high demand of connected devices.

The major challenge is secure on-boarding of trusted IoT devices i.e. Trusted network layer on-boarding, which defines each device with unique network credentials for mutual authentication,, is performed over an encrypted channel (to protect credential confidentiality) to securitize the credentials not to be accessed by anyone. This should be performed throughout the lifecycle of the devices. Understanding the above said challenges, three core elements are required to be addressed for IoT security.

- Unidentified Device Identity- vulnerable to the network
- Unreliable Data and data source and services
- Unknown custodians and captive network landing in public network

2.1.1. Unidentified Devices vulnerable to the network.

Large number of devices are expected to be connectivity enabled, ranging from wearable devices to sensors monitoring industrial processes. The challenge is now heterogeneity and the reliability of these devices, whether they will be considered as reliable or not, and thus their data will be kept for further analysis or not.

The reliability of the devices only can be justified with its unique tamper proof Identity and secure Operating system. In this context, focus should be on secure design and architecture of the devices. Weak design of connected devices, have challenges to secure the Firmware, Operating System and software assets, and even have the risk to tamper the device identity. Tampered or tamper-able device identity are presumed as unidentified and unreliable device, boon to the attackers.

2.1.2. Unreliable Data, data source and Services

As discussed in section above on unidentified devices, weak design and unprotected memory of such devices may process unreliable data in the form of unreliable logs. which may impact the reliability of data source, service quality expected from these endpoint devices and further data analysis.

Organizations need to identify the historical information they should store that will be useful to reveal trends over time. Something like a data lake architecture can be useful as a repository to store the full mass of structured, semi-structured and unstructured data in its native format. The use case is significant in Health organization and related practices.

Therefore, to ensure the device credibility, security standards should be followed. Security standards for the IoT devices are being developed in ITSAR by NCCS Bangalore and will be an integral part of TEC ERs.

Users of captive network landing in public network may be difficult to be identified.

Traceability is the key point in security. The device user may misuse the device by hiding the identity. Hence, identification of custodian and mapping with the device must be one of key-step to control unknown custodian. This is also true, working in captive network, one can land on public network without exposing the identification causing major challenges in IoT business.

IoT platforms are generally having the features like Registration, Discovery, Security, Data Management & Repository, Subscription & Notification, Application & Service Management, Communication Management and Delivery Handling, Semantics etc. Platforms should be able to detect the unknown users. In case of any misbehaviour found in the devices due to external attack like tampering of firmware/ software algorithms and security keysets, platforms should have intelligence to detect such vulnerable devices.

2.2. Requirement of trusted environment for IoT devices using secure Platform.

In view of various challenges related to IoT devices, following requirements should be addressed including implementation of ***digitally signed*** firmware, which is the next level of security that restrict the attacker to load rogue Firmware.

a. IoT/M2M Device Trust- *Identity, Authentication, and root for trust*

b. IoT/M2M data Trust – *End-to-End security framework*

c. IoT/ M2M Trusted Operation – *Trusted Remote Management and device life cycle*.

d. Application Mandatory Parameters

Device Identity with a legacy approach: IoT devices are having various types of communication technologies such as Bluetooth, 3GPP, Wi-Fi etc. as per the need of the use cases. The MAC address is used as a generic identification in most of the IoT devices and for 3GPP based devices, IMEI is being used as the device identity (more details in Annexure-I). Device manufacturers are creating their own device identity to manage their inventory such as device Serial Number. The device serial number is

considered as a superset of all identities present in the device. This is also a fact that, these identities supposed to be a supply chain identity, that are exposed and thus vulnerable.

Evolution in device Identity: To secure IoT/M2M, each connected device needs a unique identification – even before it has an IP address. Therefore, it is required to establish the root-of-trust for the device's lifecycle and should be an initial security requirement. Implementation of IoT devices for unique identification as well as authentication should be only known to the device and IoT platform.

There are several candidates for roots of trust, depending on the class of security required in the use case. RFID tags can support most low-end use cases. UICC enabled components like the ubiquitous SIM can support various classes and types of use cases.

Secure device onboarding: In view of several challenges as detailed above, the secure onboarding of IoT/ M2M devices shall be needed by the IoT platform to manage Device identity lifecycle by provisioning the secure device identities with a PKI-based platform as exceptional security. The IoT Platform with digital identity architecture with evolving specifications protects IoT devices, data, and communications from chip to cloud through encryption, authentication and authorization with secure onboarding process as listed below

a. Device Registration on IoT Platform
b. Public Key Infrastructure (PKI) based platform delivers exceptional encrypted security
c. Provisioning of secure digital certificates of ITU-T X.509, unique device identity backed by trusted Certificate Authority (CA)
d. Enables revocation services, end of life decommissioning or repurposing.
e. Delivers cloud-based functionality and security.

   This would be the strongest protection mechanism to secure the devices to ensure the architecture, verification of the integrity of the operating system and applications on the device.

2.2.1. Proposal for Composite Virtual Identity of the IoT Device

Virtual Identity of the IoT Device connected with the IoT platform is another concept/ idea for enhancing the composite identification of devices including the platform on which they are deployed.

IoT Platforms shall have additional responsibility to create composite virtual Identity to generate virtual ID and further share to NTC to identify the devices with their respective platform. The NTC shall be the repository of these composite virtual IDs. Standard hash generation algorithm may be used for composite virtual Identity.

E.g. Virtual ID = [Algorithm] {Device Certificate| Device specific Application ID |Platform ID| SIM ID}

2.2.2. IoT/M2M data Trust – Secure by design and End-to-End security framework

End-to-end encryption allows all traffic from a source to a destination to be fully encrypted and authenticated, so that if someone captures that traffic, they cannot read the inside information.

Defining in with respect to security framework, End-to-End Security means that the authentication and communication between the Device and its Application Host or its Remote Management Host is authenticated and encrypted using either Digital Certificates or Pre-shared Keys pre-provisioned on the device and exchanged securely between the device and application host for entities and actions.

- Secure communications between devices, gateway, and cloud
- Authorized software and firmware updates.

Mandatory requirement for the devices would be

a. All commands shall be encrypted or signed.

b. Secure Element can be used for end-to-end encryption / decryption within IoT devices whose low-end controllers cannot handle the high-end security features.

c. Data shall be encrypted.

d. All messages should have, replay protection and integrity checks

e. Use industry proven standard protocols or recommended by respective ITSAR

Bootstrapping, Authentication and Authorization

The bootstrapping, authentication and authorization of connected devices and applications may be as per the ITU-T Y.3056 or the oneM2M TS-0003 Security Solutions. The functional architecture as defined in ITU-T Y.3056 is reproduced. The Information flows may be considered as per ITU-T Y.3056, which includes the process of registration and transfer or as per other, such guidelines as published by sectoral authorities from time to time. For bootstrapping parameter ETSI standard ETSI TS 133 220 / ETSI TS 131 102 may be referred.

2.2.3. IoT/ M2M Trusted Operation – Trusted Remote Management and device life cycle.

The International Telecommunication Union (ITU-https://itu.int) has defined The Internet of Things (IoT) in Recommendation ITU-T Y. 2060 (06/2012) as ***a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies***.

Secure communication and remote management services as well as remote monitoring are the key elements to enable device life cycle according to its defined use case.

Remote Management

IoT Devices and Machines are uniquely identifiable, configurable, provision-able and monitor-able using remote management functionality with an Authenticated Channel by the application service provider or Service provider (as relevant) whilst operating in their

deployment locations. The provisioning of connectivity and changes in device configuration must be done using an authenticated Channel, which uses secure keys to authenticate servers to the devices and ensures that the communication is encrypted end to end.

Remote Monitoring

Secure access as specified in Remote management is conditional and limited access that can be used for Remote Monitoring. It involves collecting data from IoT devices and using this data to trigger automatic alerts and actions, such as remote diagnostics, maintenance requests, and other operational processes. By using IoT, assets located anywhere can be monitored.

What helps in secure Remote Monitoring?

i. Faster response to the equipment issues
ii. Analysis of the end-to-end business process—how it works today, where the inefficiencies are, and what changes need to made;
iii. Alerts that are to be created automatically
iv. Analysis, which helps to determine the capabilities of the system.
v. Automatic Reporting
vi. 24*7 Monitoring

2.2.4. Application Mandatory Parameters

IoT/ M2M ecosystem comprises of telecom service providers, sensors, hardware OEMs, supply chain, middleware, asset management including IoT/M2M application and application service providers.

Different types of applications have different needs in terms of network resources leading to different requirements. Identification of mandatory parameters for application is required for initial step towards the security, which leads to the tractability. Application required parameter would be-

- Application ID
- Developer information

2.2.5. Application & Service Identifier Standards

- Application and service identifiers are usually defined in the context of the specific platforms (e.g., service platform, operating system) on which they are provided. This can be standards based or proprietary. In case the platform is standardized, the application and service identifiers are also standardized.
- Examples:
    - OneM2M Application & Service Identifiers: OneM2M TS-0001 defines various identifiers that are used by OneM2M based IoT solutions. This includes identifiers for applications, application entities and common service entities.
    - For Java application or applets ETSI TS 101 220 is a standard being used to define unique application Identity.

- REST Resource Identifier: Representational State Transfer (REST) is a programming paradigm for distributed systems. It offers services by an electronic device to another electronic device using a uniform and predefined set of stateless operations. The resources of these services are identified by URIs. The URI format is defined in IETF RFC 3968.

3. Concept of National Trust Centre

Telecom Regulatory Authority of India (TRAI) in its recommendations at para 2.81 has mentioned that "In Germany, there is a neutral and independent trust centre "TÜViT[5]" for ICT. They assess security and quality characteristics against recognised criteria and standards. TÜViT evaluations and certifications create the necessary trust in IT products, systems, and processes, and in IT infrastructure. Similar to this, for testing and certification of M2M devices and applications (hardware and software), Government should create a National Trust Centre (NTC). ***Also, only certified devices should be allowed to be used in M2M communication ecosystem.***

As mentioned in chapter-1 of this report, following work items were communicated to TEC by DoT, vide L.No. 6-18/2018-Policy I dated 1st October 2018, to study and create the framework:

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

2) A National Trust Centre (NTC), under the aegis of TEC, should be created for the certification of M2M devices and applications (hardware and software). *This recommendation was accepted in principle by DoT.*

   However, DoT also decided that for certification of software products & applications related M2M devices, STQC (Standardization Testing and Quality Certification)[6] under MeitY (Ministry of Electronics and Information Technology) may be the agency to carry out such testing under single window of proposed National Trust Centre.

Both the work items are interrelated as Security by design guidelines will help in the development of secured IoT devices and the work item at point no (2) above will further ensure their credibility by means of testing and certification.

As already mentioned in chapter-1, TEC formed a multi-stake holder Working group to study and prepare the report based on global standards and international best practices.

IoT device H/W will be tested as per MTCTE Essential requirement (ER) prepared by TEC, and the software by STQC. STQC has shared some testing specifications being used for testing the software of IoT products (Annexure-III). MTCTE is already in progress and being implemented in phased manner to cover the telecom equipment and the devices.

MTCTE has already taken initiative for the development of work item mentioned at point no. (2).

As the MTCTE is in beginning stage therefore it may take time to have only the certified devices in the network. However, efforts should be made to enhance the share of certified devices in the network in near future.

There will be certified (as per MTCTE) as well as non-certified (already deployed/ not covered in MTCTE) devices in the network.

[5] https://www.tuvit.de/en/home/
[6] https://www.stqc.gov.in/software-testing-and-assessment-0

However, as per study of various global documents and discussions in the working group, it has been envisaged that vulnerabilities/ security issues may arise in any device working in the network. Vulnerabilities and security related issues detected by the IoT/ Smart city platforms should be addressed by the IoT devices manufacturers in a time bound manner.

To address the security & vulnerability related issues of M2M/ IoT devices, framework for a central entity named as National Trust Centre having connectivity with all the IoT platforms is required to be established.

Study is in progress in the TEC working group and as a part of *Security by Design principles* work item, report on ***"Code of Practice for Securing Consumer Internet of Things(IoT)***" has been released by TEC in August 2021. Guidelines available in this report will be helpful in securing consumer IoT ecosystem and also in managing vulnerabilities.

This report is intended for the use by IoT device manufacturers, Service providers / system integrators and application developers etc.

Similar guidelines have been adopted by UK in 2018, European Union (EU) in 2020, Singapore, Finland, Australia, Vietnam etc.

IoTSF in its document ***The Contemporary Use of Vulnerability Disclosure in IoT***[7] released in November 2021, has mentioned the countries working on IoT security and referred the TEC report also. Sections in this document on "Research Analysis and Development", "Recommendations from IoTSF" and "Conclusions" available on page no's 9, 18 and 19 respectively seem to be quite important from the point of view of vulnerability disclosure and security.

UK DCMS in its policy paper - ***Government response to the call for views on consumer connected product cyber security legislation***[8], published in April 2021, has mentioned that they are in the process of public consultation for mandating the following three security requirements:

- Ban Universal default password.
- Implement a means to manage reports of vulnerabilities.
- Provide transparency on for how long, at a minimum, the product will receive security updates.

Above three security requirements are in line with the **code of practice released by UK DCMS in 2018** and also similar to the first three guidelines available in ETSI TS 103 645 / ETSI EN 303 645.

Guidelines available in ***Code of practice for securing Consumer IoT*** released by TEC, India will help in creating the ecosystem of secured devices and reducing vulnerabilities. At least the first three guidelines as detailed below are required to be adopted:

[7] https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/The-Contemporary-Use-of-Vulnerability-Disclosure-in-IoT-IoTSF-Report-4-November-2021.pdf

[8] https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response/government-response-to-the-call-for-views-on-consumer-connected-product-cyber-security-legislation

(a). No universal default passwords i.e. Ban default password.

(b). Implement a means to manage reports of vulnerabilities.

(c). Keep software updated

Considering the chapter "Trusted Electronic Value Chain" of National Policy of Electronic (NPE[9]) 2019, trusted device, software (Boot loader, Operating System, Application), and even the active programming code that exists in supply chain components, should be the focus to securitise the devices.

It is therefore evident that all the IoT/M2M devices which are intended for use in the ecosystem should be got tested by the manufacturer as per MTCTE ERs (H/W testing) and by STQC (Software testing), prior to their sale / deployment, as mentioned in chapter- 1.

3.1. NTC visualization by the Working group

The National Trust Centre may be visualized as a repository that manages the lifecycle of trusted (tested & certified under MTCTE and software by STQC) M2M/ IoT devices and is expected to provide a sense of trust to the users. The trust may be built by ensuring that the M2M/ IoT devices are safe and secured and if the devices are hacked or become vulnerable, it should be detected by IoT platforms and intimated to NTC. National Trust Centre shall have the repository of uniquely identified trusted IoT devices, Apps & IoT device manufacturers, will get these vulnerabilities addressed by the device manufacturers

The following stakeholders that create the secure ecosystem are required to be addressed:

- IoT/ M2M device manufacturers
- Secure Element / SIM/eSIM provider.
- IoT data and remote management services
- Telecom Service Providers
- Controllers of Certificates
- Certifying Authorities e.g. the accredited labs for testing & certification of devices & applications
- IoT/M2M Service Providers (including platform provider),
- IoT/ M2M Applications
- IoT/ M2M Application providers
- Device owner and application users
- IoT Registrars of other countries, Security Agencies and Sectoral Registrars e.g., VAHAN portal of MoRTH for Connected Vehicles in India

NTC should have the repository of certified devices as well as the related manufacturers from MTCTE portal and the uncertified devices by way of registering the device manufacturers.

However, efforts may be made to create repository through the process as described in para 2.2.1.

The repository should also have the record of vulnerabilities communicated by IoT/ Smart city platform as discovered in the certified / non-certified devices time to time to provide a mechanism of continuous improvement in safety and security of the devices and the networks. These vulnerabilities should be communicated to the related stakeholders to address it and also to upgrade the software / firmware as required in the same model of devices deployed in the eco system.

Important requirements for creating the framework of NTC and the conceptual diagram inline are as given below:

- Registration of M2M Service Providers
  - Registration Authorities for M2M Service Providers may be TEC (DoT).
- Registration of M2M Application Service Providers
  - Registration Authorities for sector specific Applications, and the Application Service Providers may be MEITY/ ISGM / MCI / MoRTH etc
- Registration of Certified Connected Devices
  - Integration with the MTCTE Registry of Certified Device Manufacturers
  - Integration with sectoral device certification registries like MoRTH for VTS
- Registry of M2M Applications
  - Sectoral App registries, interfaces, and protocols as per global standards
  - Federation of databases of various registration authorities
- Registry of tamper resistant end point identifiers
  - Subscriber and Network identity lists from various TSPs, ISPs and M2M Connectivity providers (including LoRa, Z-Wave, ZIGBEE, etc.)
- Security and Testing Certifications
  - Product life cycle security
  - Supply chain security (Product development to end customer)
  - Software (OS and Security implementation)

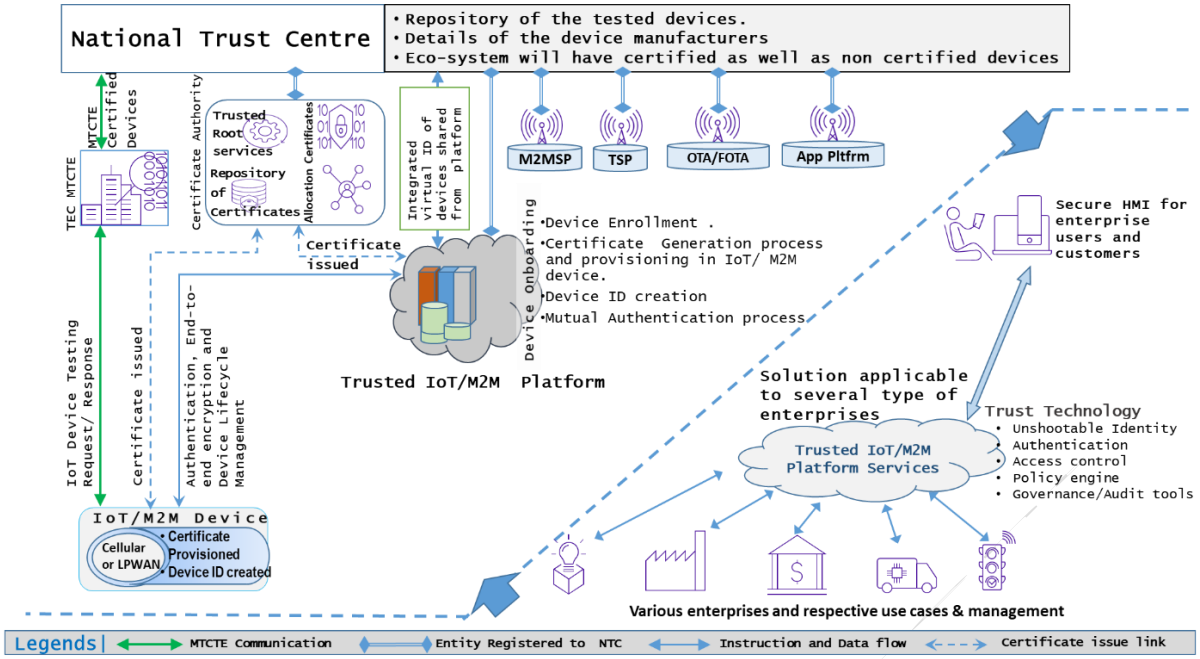


Figure-1: Conceptual diagram of National Trust Centre

3.2. NTC – proposed plan and related activities

National Trust Centre is a new concept, and it has not been found in any standard / documents available on the web. It will be evolving with time, therefore needs to be implemented in phases.

Phase 1:

Proposed activities for phase -1 are as listed below

i. Creation of NTC Portal (To begin with MTCTE portal may be used)

ii. Creating repositories of certified devices (tested under MTCTE) and related manufacturers

iii. Registration of various entities of the IoT eco-system (M2M Service provider including platform, Application provider, Secure element provider etc.) on DoT portal and securely transfer the related details to NTC portal

iv. Registration of IoT device manufacturers, whose devices are already working in the networks and presently not covered in MTCTE (policy intervention required to register such IoT devices manufacturers at DoT portal/ NTC portal).

Platforms may send the connected devices details to the NTC portal as per the process mentioned in section 2.2.1.

v. Pilot with IoT service providers (scope may be defined separately)

Phase 2:

Proposed activities for phase -2 are as listed below

i. IoT device manufacturers whose devices' samples have been certified in MTCTE, shall enter details of the devices expected to be deployed in the network

ii. Develop vulnerability disclosure policy for IoT device manufacturers/ application providers

iii. Requirement for issuing Unique identity for the platforms registered by DoT

iv. Communication between platform and the NTC in a standardised format

v. Addressing vulnerabilities through manufacturers

vi. Exploring options for empanelling the researchers

Phase 3:

Proposed activities for phase -3 are as listed below

i. Custodian registration at the NTC for specified set of mission critical use cases involving a minimum level of assurance (will require the policy intervention)

ii. monitoring of devices as per agreed SLA (will require the policy intervention)

iii. Limiting access of black-listed devices via their respective IoT platforms (will require the policy intervention)

iv. Template for device registration data from sectoral registrar database to NTC as per the agreed SLA for the use case belonging to specific sector. (will require the policy intervention)

3.2.1. NTC framework

The NTC may have the following main interfaces:

- Interface with TEC MTCTE (Mandatory Testing and Certification of Telecom Equipment) portal to have access to the lists of certified manufacturers of connected devices.
- Interfaces with sectoral registrars that maintain lists of certified manufacturers and service providers (e.g. Vehicle Registry of MoRTH (Ministry of Road Transport & Highways))
- Interfaces with Global App Repositories to maintain a white / black list of global device and application providers
- Interfaces to Indian security agencies including but not limited to CERT to offer a centralised view of Certified Devices and Applications, and to be able to assist in identification of rogue devices and applications.

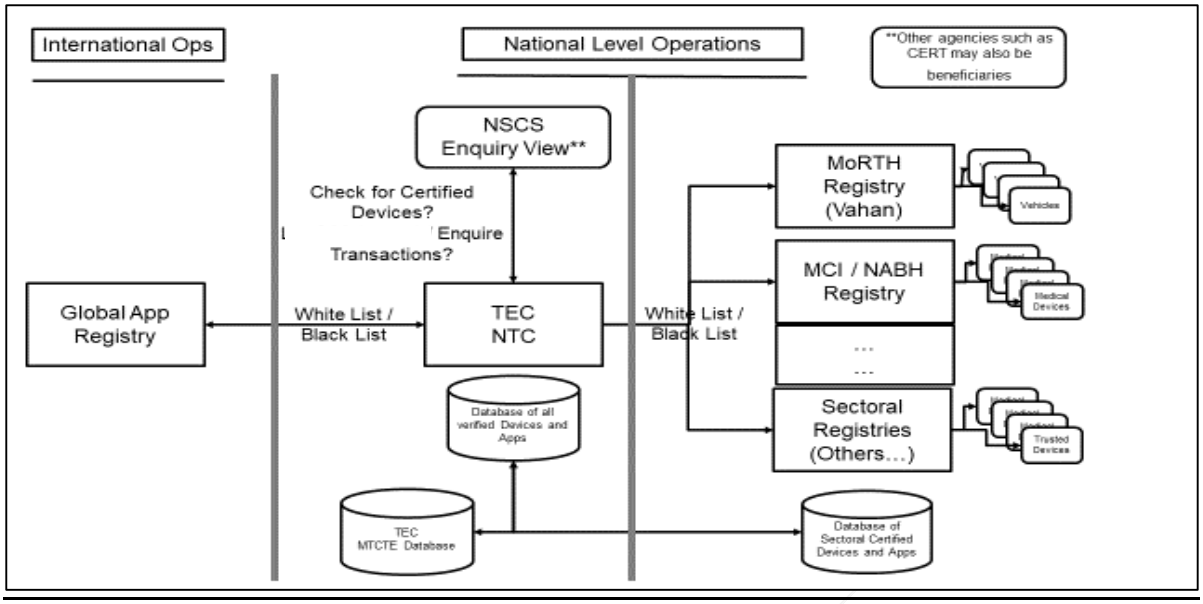


Figure-2: Block diagram of National Trust Centre

National Trust Centre should share the data with MTCTE server, CERT and the IoT / Smart City platforms. For maintaining trust, it is required that the trust centre which will be a central entity, should ensure that vulnerabilities are addressed in time by the manufacturers. In case of delay, rogue devices may be disabled by the M2M Service provider / platform.

NTC will have the repository of the tested devices. Details of the manufacturers certified under MTCTE as well as not covered under MTCTE.

Eco system will have certified as well as non-certified devices.

If vulnerability arises in any of the device, platform should detect and intimate to NTC along with the details such as platform ID, device type, manufacturer, model etc. For this, provision in the portal may be made. Portal will find out the manufacturer from the repository and communicate vulnerability. Some researchers may be empanelled by TEC to study and mitigate vulnerabilities.

For having secured devices in the ecosystem, manufacturer should design the devices with built in security features.

NTC will expose the repository of certified devices to the registered M2M/ IoT service providers (Platforms).

IoT Platform should have the facility to digitally allow or deny devices by validating the certificates during on boarding of the devices.

3.2.2. NTC portal

A TEC NTC portal needs to be designed for handling all the work related to registration of IoT/M2M devices/ network elements, equipment manufacturers, secure element manufacturers, app providers, service providers, registration of practice statement, trust computation, certification, and life cycle management of entities. The portal will

serve as the common platform to bring together all the entities and relevant stakeholders.

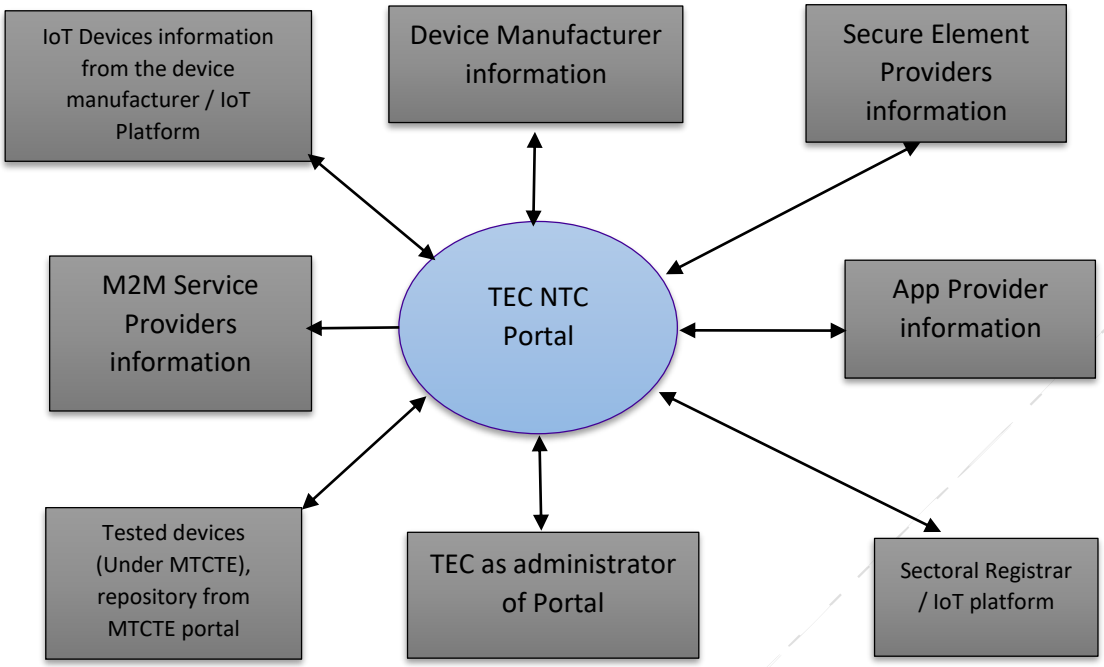


Figure-3: National Trust Centre Portal

Various features of the portal should be:

1. Registration / information of all entities
2. Data management and analytics
3. Online tracking of applications
4. MIS
5. System for logging and history of tickets of various kinds
6. Discussions and chatrooms can be made available so that stakeholders can contact each other.
7. Helpdesk support to all the stakeholders or member countries.

The entities mentioned in the M2M service provider registration policy will register on DoT portal & NTC will pull the information from that portal.

4. Policy intervention required for the development of NTC

1. As mentioned in the Chapter -1 and 3, IoT device H/W is to be tested under MTCTE regime and software by STQC. M2M/ IoT devices having / expected to have larger share in the networks are required to be covered in MTCTE for H/W as well as S/W testing to increase the share of certified devices in the network. MTCTE portal should register the M2M/ IoT device manufacturer as per the specified template and have a repository of device manufacturers and certified devices.

Action by DDG(MTCTE) TEC

2. Registration of M2M/ IoT Service Providers. All the platforms should be given unique identity no. to be recognised by NTC.

Policy matter: Action by DDG NT, DoT

3. All the M2M/ IoT device manufacturers whose devices are working in the network or being deployed and not covered under MTCTE, should register on DoT / NTC portal. (Manufacturer detail, device type, model unique id etc.)

Policy matter: Action by DDG NT, DoT

4. M2M/ IoT devices manufacturers should be mandated to have a means of vulnerability disclosure policy to be declared on their portal. (As referred in code of practice for securing consumer IoT). Case has already been sent to DoT.

Action by DDG SA DoT

5. Since different devices may be subject to different levels of security risks, therefore, devices will be required to be classified depending upon the risk associated with the application. This may be considered as an important aspect while developing security specifications for IoT devices in ITSAR.

Action by NCCS Bangalore

6. As IoT is a globally connected domain, therefore the globally unique identifiers developed by global SDOs should be used. Some of the identifiers with example are available in Annexure-I.

Action by TEC

7. NTC should establish connectivity with related CERTs for synchronization of data and generating vulnerability identification from CERT-IN.

Action by TEC

Annexure-I: IoT Identifier

IoT Identifier[10]:- The notion of object identification is already extensively used for things in the physical world, such as desktop computers, servers, mobile devices, networking devices (e.g., routers, switches, hubs), network interface cards, energy meters, sensing devices, actuating components, RFID/AutoID readers, tagged items/products, application gateways and more. All these physical objects are associated with an identifier such as a hostname, an IP address, or a URI (Universal Resource Identifier).

At its full scale, the emerging IoT paradigm foresees flexible and transparent interactions across numerous physical and logical objects. This requires identification systems that can address the full range of physical and logical/virtual objects outlined above. The identification technologies and solutions outlined above provide a sound basis for IoT identification and are already used in the scope of several IoT applications.

IoT Identifier Type	Examples
Application IDs	URIs, URL
Communication IDs	IPv4, IPv6, E.164
Object IDs	EPC, UPC, Handle/DOI, UUID, MAC, URI, URL, Ecode, OID, CID

In IoT systems multiple identifiers are used. They identify different or the same entity and belong to multiple classes. An example in the context of smart phone is given below:

Smart phone: In smart phone multiple identifiers are used which are directly or indirectly related to the smart phone, user, subscriber and other purposes. Note that the list is not necessarily complete and that not all listed identifiers are relevant for a specific IoT application. Some identifiers are as:

Device Identifier (Device ID) or serial number is a unique identifier for the smart phone and assigned by the vendor of the system software. It is for example used for the device identification in USB communication. The Device ID is a thing identifier.

International Mobile Equipment Identity (IMEI) is a unique identifier for mobile phones (3GPP based networks). It is used by the mobile network to identify the specific smart phone and can for example be used to identify stolen devices. It has no relation to the subscriber. It consists of 15 digits starting with an 8-digit Type Allocation Code (TAC) which identifies the mobile phone type followed by the 6 digit serial number and an optional 1 digit checksum. The TAC is assigned by organizations that are approved by the GSM Association and the first 2 digits of the TAC indicate the organization. The IMEI is a thing identifier.

-

International Mobile Subscriber Identity (IMSI) identifies the subscriber on the mobile network. The IMSI is stored on the SIM card. It is usually a 15-digit number with 3 digits for the Mobile Country Code (MCC) and 2 or 3 digits for the Mobile Network Code (MNC). The

[10] https://www.iot6.eu/sites/default/files/imageblock/EU-China_IOT-ID-White-Paper-V1.0-Final.pdf

reminder is the Mobile Subscription Identification Number (MSIN). The MCC is assigned by ITU and the MNC by country specific authorities (e.g., regulator). The IMSI is a user identifier.
-

Mobile Station ISDN Number (MSISDN) is the phone number of the subscriber which has to be dialled in order to call it. A subscriber can have multiple MSISDN but only on IMSI. The MSISDN is a communication identifier.

Integrated Circuit Card Identifier (ICCID) is the identifier of the SIM card itself. The ICCID is a thing identifier.

Hostname of the smart phone for the internet connection via the wireless LAN interface. Hostname is a communication identifier. IP addresses for network connections when the smart phone is connected to the internet. The IP address is a communication identifier.

MAC address of the wireless LAN interface is a communication identifier.

- Bluetooth device address of the Bluetooth interface is a communication identifier.

- Near Field Communication (NFC) identifier of the NFC interface is a communication identifier.

Android ID (aka SSAID for Settings. Secure ANDROID_ID) is generated on first setup of a smart phone (also after factory reset) and identifies the user account. In case of multiple user accounts on a device each account has its unique Android ID. The Android ID is a user identifier.

Usernames for specific applications (e.g., Google applications, email, messenger)

User names are user identifiers.

- iOS Application ID and Android Application Package ID are identifiers for smart phone applications.

- iOS Application ID and the Android Application Package ID are application identifiers

Vendor specific identifier for advertising purposes like Android Advertising ID, Apple Identifier for Advertising, Windows Advertising ID.

Advertising identifiers are application specific identifiers.

Annexure-II: Definitions

(i) **M2M/ IoT Device manufacturers:** Entities that create an assembled final consumer M2M/ IoT product, which is likely to contain the products and components of many other suppliers.

(ii) **Mobile Application Developers:** Entities that develop and provide applications that run on devices. These are often offered as a way of interacting with devices as part of an IoT solution.

(iii) **M2M/ IoT Service Providers / System integrators:** Companies that provide services such as networks, cloud storage and data transfer which are packaged as part of IoT solutions. Internet-connected devices may be offered as part of the service.

(iv) **Consumers:** Consumers may take many forms. Governments, businesses and individuals may all be consumers of IoT devices. This Code of Practice particularly focuses on consumer grade, internet-connected devices and associated applications (e.g. wearable devices, and home appliances such as "smart" televisions and refrigerators).

(v) **Retailers:** The sellers of internet-connected products and associated services to consumers.

(vi) **Device ID provider:** Standardized unique Device ID is important to identify the device; this improves the traceability, controls, and use-cases of devices. Secure identity based on X.509 is recommended. Please see above under "Device Identity and certifications. As discussed above Device serial no maps with Transmission technology (IMEI for GSM and 3GPP, MEID for 3GPP2, Mac for BLE, Wi-Fi and LPWAN) in build in the device. Device ID provide shall be a global standardised body. Without Identification, device cannot be registered in public network. While registering to NTC, device manufacturer has to define device serial number mapped with Transmission technologies IDs.

(vii) **IoT Gateway:** A unit in the Internet of things which interconnects the devices with the communication networks. It performs the necessary translation between the protocols used in the communication networks and those used by devices.

(viii) **MTCTE (Mandatory testing and Certification of Telecom Equipment):** Department of Telecommunications, Ministry of Communications has notified "Indian Telegraph (Amendment) Rules" in Gazette of India vide G.S.R. 1131(E) PART XI" on 5th September 2017 which prescribes for Mandatory Testing and Certification of Telecommunication Equipment. Any telegraph which is used or capable of being used with any telegraph established, maintained or worked under the license granted by the Central Government in accordance with the provisions of section 4 of the Indian Telegraph Act, 1885 (hereinafter referred to as the said Act), shall have to undergo prior mandatory testing and certification in respect of parameters as determined by the telegraph authority from time to time.

(ix) **IoT:** ITU-T in its Recommendation ITU-T Y.2060 (06/2012)[11] has defined Internet of Things (IoT), as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

(x) **ITU-T X.509 -** ITU-T X.509 | ISO/IEC 9594-8 defines frameworks for public-key infrastructure (PKI) and privilege management infrastructure (PMI). It introduces the basic concept of asymmetric cryptographic techniques. It specifies the following data types: public-key certificate, attribute certificate, certificate revocation list (CRL) and attribute certificate revocation list (ACRL). It also defines several certificates and CRL extensions, and it defines directory schema information allowing PKI and PMI related data to be stored in a directory. In addition, it defines entity types, such as certification authority (CA), attribute authority (AA), relying party, privilege verifier, trust broker and trust anchor. It specifies the principles for certificate validation, validation path, certificate policy etc. It includes a specification for authorization validation lists that allow for fast validation and restrictions on communications.

[11] https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060

Annexure-III: Testing specifications for IoT device software shared by STQC

The security evaluation requirements for all the evaluation activities have been derived from the respective OWASP guidelines as mentioned below:

Firmware (running on device) - OWASP Application Security Verification Standard 4.0 [Appendix C: Internet of Things Verification Requirements] https://owasp.org/www-pdf-archive/OWASP_Application_Security_Verification_Standard_4.0-en.pdf (Page no.66)

Mobile application (used in IoT ecosystem) - OWASP Top 10 Mobile Risks 2016 https://owasp.org/www-project-mobile-top-10/2016-risks/

Web application (used in IoT ecosystem) - OWASP Top 10 Risks 2017 https://owasp.org/www-project-top-ten/2017/Top_10

Web APIs (used in IoT ecosystem) - OWASP API Security Top 10 2019 https://owasp.org/www-project-api-security/

Annexure-IV: Root of trust

The root of trust is the key element on which all secure operations depend. It contains the keys used for cryptographic functions and enables a secure process. It is inherently trusted, and therefore must be followed in secure by design architecture of the trusted device.

This follows the principle of the hardware security module (HSM) which generates and protects keys and performs cryptographic functions within its secure environment. The ecosystem can trust the cryptographic algorithm, keys and data received as an authentic and authorized information from the root of trust module. Basic functionalities of root of trust are as below:

- Globally unique and inter-operable identity
- Tamper resistant Root of Trust
- Root of trust attributes available in digital form/ electronic form factor
- Easy to use, easy to integrate into devices
- Small form factor, frugal in cost
- Widely available
- Industrial grade, long life
- Remote manageable and remote Provisionable
- Possible to be certified as per global standards
- Easy to be issued by existing trust providers and registrars
- Easy to securely relate with a national identity
- Possible to registered in a Trust centre

Bootstrapping

This interface assures the Mutual Authentication and Authorization of security nodes belonging to service providers, application providers and registrars using online and real time systems. ITU-T Recommendation *Y.3056 Framework for bootstrapping of devices and applications for open access to trusted services in distributed eco system* may be referred.

Some interfaces required with the NTC are as given below:

1. Lawful Interception- Status Update

This interface permits the NTC to make an enquiry to the Sectorial or International Registrar to check/ update the status of the Device/ App (White/ Grey/ Black)

This interface permits the NTC to make an enquiry regarding the validity of the Device/ App Certificate/ Location/Validity etc.

2. Accreditation of Certified Devices and Applications

This interface assures the registration of Service Providers, Application Providers and Device Manufacturers to the respective trust authorities, registrars (Telecom Service Providers, Machine to Machine Service Providers, Application Service Providers)

3. Registration of root of trust based Certified Devices and Apps

Upon the successful certification of a make and model, the OEM/ ASP uses this interface for the Registration of root of trust based certified Devices and Apps that are manufactured/ installed by the OEM/ ASP

4. Certification of Devices and Apps as per Specifications

This interface assures the recording of the Mandatory testing and certification of connected devices and applications by the Original Equipment Manufacturer (or the person importing telegraph (device) for sale in India)

5. IoT ASP and NTC Interface

This interface is responsible for discovering, recording and escalating the abnormal device / device data behaviour

6. Device and ASP interface

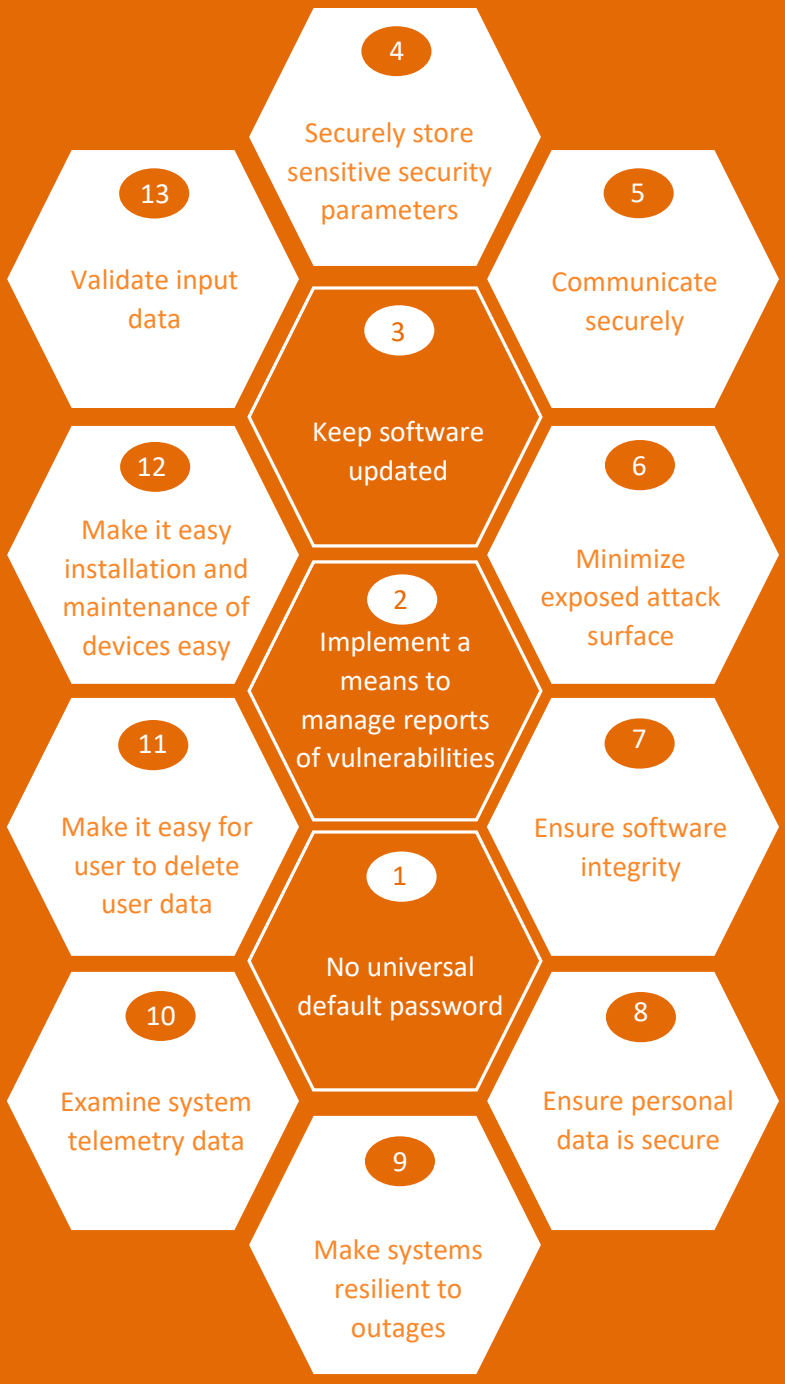
This interface assures the frequent and regular mutual authentication between devices and the servers receiving and hosting the data from the device. It also assures the Remote management and configuration shall be compliant to national and international standards like ETSI TS 101 181 V8.9.0 or OMA DM (wireless) or BBF TR-69 (wireline).

Identities and information elements that are private and sensitive to users, networks or service providers shall be transported encrypted and transformed such that the real identities are only known to the party that owns the private data and not to agencies that are transporting or processing the information.

7. Certificate and Keys Management Authority Interface

This interface is responsible for provisioning and verification of Keys and Certificates to IoT SP, ASP and Device OEMs

There may be more stakeholders and therefore many additional interfaces which may later be added to the diagram and the list above.



ISO 9001 :2015

TELECOMMUNICATION ENGINEERING CENTRE
DEPARTMENT OF TELECOMMUNICATIONS
MINISTRY OF COMMUNICATIONS
GOVERNMENT OF INDIA