सत्यमेव जयते

TECHNICAL REPORT

Recommendations for IoT / M2M Security

TEC-TR-SN-M2M-009-01

M2M SECURITY WORK GROUP

ISO 9001:2008

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

RELEASE 1.0

January, 2019

IoT / M2M Security Work Group Technical Report

Document Number	TEC-TR-SN-M2M-009 – Release 01
Document Name:	Recommendations for IoT / M2M Security, IoT / M2M Security Work Group
Date:	Tuesday, 8th January, 2019
Objective:	This Technical Report examines the principles and approaches for enabling security in IoT / M2M solution domain and prepares the recommendations for way forward

Sub Group 1 Lead Person Cum Coordinator	Mr. Vikas Phogat	Idemia
Sub Group 2 Lead Person Cum Coordinator	Mr. Sumit Monga	Unlimit
Sub Group 3 Lead Person Cum Coordinator	Mr. Sharad Arora	Sensorise Digital
Sub Group 4 Lead Person Cum Coordinator	Dr. Vijay Madan	TSDSI
Sub Group 5 Lead Person Cum Coordinator	Mr. Aurindam Bhattacharya	C-DOT

Government of India
Ministry of Communications, Department of Telecommunications
Telecommunication Engineering Centre

www.tec.gov.in

Revision History

Date	Release	Document No.	Description
08/01/2019	Rel 01	TEC-TR-SN-M2M -009	Technical Report on principles and approaches for enablement of security in IOT/M2M domain and recommendations.

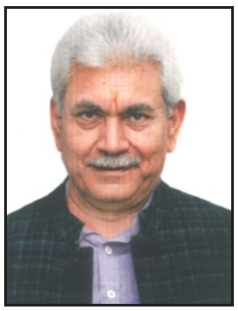
Important Notice

Individual copies of the present document can be downloaded from http://www.tec.gov.in Users of the present document should be aware that the document may be subject to revision or change of status.

Any comments/suggestions may please be sent to: adgsn.tec-dot@gov.in

Disclaimer

The information contained is mostly compiled from different sources and no claim is being made for it being original. Every care has been taken to provide the correct and up to date information along with reference 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.



मनोज सिन्हा
MANOJ SINHA
संचार राज्य मंत्री (स्वतंत्र प्रभार)
एवं
रेल राज्य मंत्री, भारत सरकार
Minister of State (Independent Charge)
for Communications
and
Minister of State for Railways
Government of India

MESSAGE

I am glad to note that the Telecommunication Engineering Centre is publishing a Technical Report on IOT/M2M Security.

IOT/M2M communication is poised to change the way humans live, and enable us to control our surroundings as well as the various social and economic sectors which operate around us. It is expected to improve the efficiency of sectors such as Automotive, Health, Power, Safety & Surveillance etc. by transmitting information/data electronically, automating the processing of information/data, and data analytics which will help in improving the quality of services to our citizens.

I am confident that this Technical Report will help in developing specifications/standards to be used in India for IOT/M2M communications security, and provide an opportunity for manufacturing a wide variety of secure and safe devices in India. I congratulate TEC and all concerned for this commendable and timely work, and wish them success in their endeavours.

Manoj Sinha

(MANOJ SINHA)

Room No. 105, Sanchar Bhawan, 20 Ashoka Road, New Delhi - 110 001
Phone : 91-11-23739191, 23372177 Fax : 91-11-23723330

अरूणा सुंदरराजन, आई.ए.एस
सचिव
Aruna Sundararajan, I.A.S.
Secretary

सत्यमेव जयते

भारत सरकार
संचार मंत्रालय
दूरसंचार विभाग
Government of India
Ministry of Communications
Department of Telecommunications

MESSAGE

I am extremely happy to note that Telecommunication Engineering Centre (TEC) is bringing out Technical Report regarding security in IOT/M2M.

This report on IOT/M2M security, which has seen active contribution from the concerned stakeholders of the industry, is very timely and provides in depth knowledge about the various security aspects which will have an impact on the various IOT/M2M services to be provided in future and will greatly benefit all the concerned stakeholders.

India's digital economy is expected to reach one trillion USD by 2025. As per National Digital Communication Policy, the IOT ecosystem is targeted to expand to 5 Billion connected devices by 2022. One of the three missions of NDCP 2018, is Secure India which requires ensuring Sovereignty, Safety and Security of Digital Communication.

To secure effectively India's economic, social and political interests, its "digital sovereignty" encompassing the data privacy and security of its citizens requires to be kept in prime consideration. To this end the Technical Report on Security in IOT/M2M is a welcome and much awaited step in this direction.

India has to make strides in making its various sectors and cities smart for which quick adoption of secure IOT/M2M is the necessary. This report will help stakeholders in development and finalization of sectors specific plans for adoption of secure IOT/M2M services.

I appreciate the efforts put in by Telecommunication Engineering Centre in bringing out this report. I wish them success in all their endeavors.

(Aruna Sundararajan)

संचार भवन, २०, अशोक रोड, नई दिल्ली - ११०००१ / Sanchar Bhawan, 20, Ashoka Road, New Delhi-110001
Tel. : 011-23719898 Fax : 011-23711514, E-mail : secy-dot@nic.in

एन. सिवासैलम, भा.प्र.से.
N. Sivasailam, IAS
विशेष सचिव / **Special Secretary**

सत्यमेव जयते

भारत सरकार
संचार मंत्रालय,
दूरसंचार विभाग
GOVERNMENT OF INDIA
MINISTRY OF COMMUNICATIONS
DEPARTMENT OF TELECOMMUNICATIONS

I am extremely happy to note that Telecommunication Engineering Centre (TEC) is bringing out Technical Report regarding security in IOT/M2M, which has seen active contribution from the concerned stakeholders of the industry, and also relentless efforts by TEC's Security Working Group (SWG) and Smart Networks Division(SND).

NDCP 2018 recognises Data as a crucial economic resource. Of the three Missions in NDCP 2018, one is SECURE INDIA – to secure the interests of citizens and safeguard the digital sovereignty of India ensuring individual autonomy and choice, data ownership, privacy and security.

This report on IOT/M2M Security brings out various aspects of IOT / M2M security, security principles of device Identification, Authentication Authorization and IOT Trust framework in a lucid way. This is important because, while M2M endpoints and M2M gateways might be dedicated to specific M2M services, M2M system as a whole will share resources with a variety of other unrelated systems and applications which have to be trusted.

This report could not have been more timely and I congratulate TEC's IOT/M2M Security Working Group and Smart Networks Division in bringing out this report which I am sure will benefit all the stake holders in the IOT / M2M domain.

N. Sivasailam

(N. SIVASAILAM)

Date: 13-11-2018

318, संचार भवन, 20, अशोक रोड़, नई दिल्ली-110 001 दूरभाष : +91-11-23717300, फैक्स : +91-11-23350495 ई-मेल : ast-dot@nic.in
318, Sanchar Bhawan, 20, Ashoka Road, New Delhi-110 001 Ph.: +91-11-23717300, Fax : +91-11-23350495 E-mail : ast-dot@nic.in

रवि कान्त
सदस्य (सेवाऐं)
RAVI KANT
Member (Services)

सत्यमेव जयते

भारत सरकार
संचार मंत्रालय
दूर संचार आयोग, दूर संचार विभाग
संचार भवन, 20, अशोका रोड़, नई दिल्ली-110001
Government of India
Ministry of Communications
Telecommunications Commission
Department of Telecommunications
Sanchar Bhawan, 20, Ashoka Road,
New Delhi - 110001
Ph.: 23714644 • Fax : 23755172
E-mail : members-dot@nic.in

I am happy to note that Telecommunication Engineering Centre (TEC) is bringing out technical report on IOT/M2M Security. We are aware that adoption of secure IOT/M2M communication will inter-alia, lead to enhancement in the safety and efficiency of various sectors of society and economy.

Need for improvement in efficiency in various socio-economic sectors has been felt for a long time and to this effect effort in this direction have also been made whereby M2M based system have been deployed. However, the solutions which have been implemented are generally based on propriety platforms. However, especially after the launch of smart cities project by Government of India, to achieve smart processes and functioning in all the sectors, interoperability of devices/platforms/applications in a secure manner is necessary which entails adoption of open but secure standards.

One of the goals of NDCP 2018, is to accelerate transition to Industry 4.0 by developing framework for accelerated deployment of M2M services while safeguarding security and interception for M2M devices and to enforce accountability through appropriate institutional mechanisms to assure citizens of safe and secure digital communications infrastructure services.

This technical report on IOT/M2M security of TEC is a good step in this direction and will certainly help various stakeholders to take preparatory steps in their respective sectors for future adoption of secure IOT/M2M communications.

(RAVI KANT)
Member (Services)

हिन्दी का मान : राष्ट्र का सम्मान

सत्यमेव जयते

भारत सरकार
संचार मंत्रालय,
दूरसंचार विभाग
संचार भवन, 20, अशोका रोड़,
नई दिल्ली-110 001
Government of India
Ministry of Communications
Department of Telecommunications
Sanchar Bhawan, 20, Ashoka Road,
New Delhi - 110 001
WEBSITE : www.dot.gov.in

MESSAGE

I am pleased to note that Telecommunication Engineering Centre (TEC) is bringing out Technical Report on Security in IOT/M2M, by virtue of relentless efforts of TEC and its Working Group on Security consisting of various stake holders.

M2M communication is an opportunity for India not only to keep pace with the world but also to march ahead in development of specifications of new and secure products consisting of Devices, Gateways and Platforms which shall be meeting the Indian requirements, though of course, in sync with the standards.

IOT Ecosystem is made up of large number of participating entities and organization. One of the main requirements of IOT Ecosystem is that each organization must individually certify that every other participating organization is worthy of its trust. The trusted ICT infrastructure comprises objects from the physical domain, the cyber domain (virtual objects) and the social domain (humans and attached devices), which are capable of being identified and integrated into ICT networks through various security components and mechanisms, which the present document on Security in IOT/M2M attempts to address.

I appreciate the efforts of Telecommunication Engineering Centre specially its SN Division and the Working Group on Security for bringing out this well awaited technical report on security in IOT/M2M domain in a very lucid manner. I wish them success in all their endeavours.

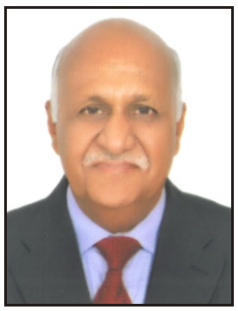
(S.S. Singh)
Member (Technology)
13.11.2018

M.P. Singhal
वरिष्ठ उप महानिदेशक
Sr. Deputy Director General
Tele : 23320252 Fax : 23329088
e-mail : srddg.tec@gov.in
www.tec.gov.in

सत्यमेव जयते

भारत सरकार
दूरसंचार विभाग
दूरसंचार अभियांत्रिकी केन्द्र
खुर्शीद लाल भवन, जनपथ, नई दिल्ली–110001

Government of India
Department of Telecommunications
Telecom Engineering Centre
Khurshid Lal Bhawan, Janpath, New Delhi-110001
ISO 9001:2008



MESSAGE

TEC is a technical body representing the interest of Department of Telecom, Government of India. It provides technical support to DoT and prepare specifications and standards for Telecom network equipment, services and interoperability including for M2M/IoT domain. TEC has also been mandated to interact with multilateral agencies like APT, ETSI and ITU etc. for standardisation.

TEC proactively takes up development of specifications & standards based on studies and on interaction with concerned stakeholders. Development of specifications & standards is a transparent process with active participation of stakeholders. Certification of telecom products as per Essential Requirements is also one of its major activities under MTCTE, which has been mandated by Government of India.

M2M systems have been in use for some time past in various sectors such as Automotive, Health Industrial sectors etc. However, the use of M2M/IoT technology, devices & application are generally proprietary in nature as standards have started involving in the recent past. It is well known fact that a variety of social and economic activities are interwoven in today's digital world, and it is possible to link them through networks and applications to achieve greater efficiency and development of new services. This can be achieved through interoperability among M2M/IoT devices, networks & applications in a secure manner, which will require standardization and development of harmonized specifications.

Towards achieving this objective, TEC in consultation with stake-holders from government, industry, standards bodies and sector-users, took up study of Security in IOT/M2M domain. Five working sub-groups were formed with the participation from stakeholders. Also a Joint Working Group under the chairmanship of Sr. Deputy Director General & Head of TEC was constituted. To assist in bringing out the report JWG secretariat has been formed along with the Editorial and the Advisory group.

Beginning the year 2017, these subgroups have worked relentlessly. This can be gauged from the fact that there were about 20 conference calls and three Face to Face (F2F) meetings and many more informal discussions, combined of all subgroups and a lot many interactions within the groups. Smart Network Divisions of TEC coordinated and managed the entire activity of formation of working subgroups, holding meetings both formal as well as informal, preparations of the reports etc.

The reports contain use cases in the sectors & their analysis with respect to security classifications, key challenges in implementation and the way forward. The report contains the suggestions in its Way-forward section which requires action by various stake holders including TEC and DoT. I express my sincere thanks to all the members of subgroups as well as members of the Security Working Group and also to all the participating stakeholders as organization and in their personal capacity whose enthusiastic support and untiring efforts have made it possible to bring out this detailed technical report in IOT/M2M security.

The report provides relevant and reliable guidance to the Industry stakeholders by citing many practical Use Case examples that can be applied to most Industry verticals, in order to plan standardized IoT deployments in a secure and sustainable manner. It also sets the foundation for the onerous responsibility within TEC to set up the National Trust Centre including the compliance to the arriving regulations in relation to privacy. I hope that the working group members and industry stake holders will provide their continued support to TEC to carry out further study and work in IOT/M2M security domain, as per the scope mandated to it by Tec/DoT, which will continually enrich our knowledge, systems and processes, such that the country can take a leadership position in the emerging global IoT Economy and Ecosystem.

(M.P. Singhal)

About TEC

TEC is a technical body representing the interest of Department of Telecom, Government of India. TEC prepares specification of common standards with regard to Telecom network equipment, services and interoperability. It releases Specifications as Generic Requirements (GRs), Interface Requirements (IRs) and Service Requirements (SR) and also issues Interface Approvals, Certificate of Approvals, and Service Approvals & Type Approvals. TEC also formulates Standards and Fundamental Technical Plans.

TEC also prepares ER's (Essential Requirements) for Telecom Equipment which has to be mandatorily complied with, as per the Indian Telegraph (Amendments) Rules, 2017, which mandates that every Telecom equipment must undergo mandatory testing and certification prior to sale, import for use in India. The application for certification under MTCTE is to be submitted online, through MTCTE portal (https://www.mtcte.tec.gov.in/) for which online administration of this procedure is being worked out.

TEC has also been appointed as the Designating Authority (DA) on behalf of DoT for Telecom Equipment. TEC as DA is designating Conformity Assessment Bodies (CAB's) / Certification Bodies (CB's) located in India to perform testing and certification of Telecom products. TEC as DA is also recognizing Foreign CAB's / CB's located in the territory of MRA partner to perform testing and certification of Telecom products to India's requirement. As of December 2018, 31 testing Labs have been designated as CAB's for testing and certification of Telecom products.

TEC also interacts with multilateral agencies like APT, ETSI, IEEE and ITU etc. for standardization, to develop expertise to imbibe the latest technologies and results of R&D. It provides technical support to DoT and technical advice to TRAI & TDSAT, and also coordinates with C-DOT on the technological developments in the Telecom Sector for policy planning by DoT. TEC also develops technical reports and specifications which address the need for standardization of Telecoms and related infrastructure within India.

About the M2M Security Work group and Sub Work group

A Work Group has been constituted by TEC to prepare a technical report on the subject of M2M Security. Accordingly, five sub groups have been formed after due deliberations with the members and consultation with the Chairman and Secretariat of the Workgroup. The issues to be taken up/scope to be defined by various sub-groups include preparing recommendations on the following:

1. Incorporation of minimal security standards for M2M products and services with interoperability in view.
2. Define guidelines from security angle with respect to
    - Data ownership and retention period
    - Security of sensitive data
    - Location of application services
    - Location of remote terminal unit/M2M devices
    - Location of core n/w elements.
3. Define policy/standards from security angle to connect legacy and non-IP devices on existing n/w technologies
4. Define precautions/security conditions for voice/SMS/MMS/video on M2M.
5. Aspects to be taken care of with respect to security framework for various verticals and solutions.
6. Define separate KYC norms for M2M from security angle.
7. Requirement of M2M product certification from security point of view

Published TEC Technical Reports or Specifications should be obtained from TEC's Publications Offices.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. TEC OR THE CONTRIBUTING MEMEBERS SHALL NOT BE LIABLE WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL THEY BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. TEC EXPRESSLY ADVISES ANY AND ALL USE OF OR RELIANCE UPON THIS INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

Copyright Notification

Contents

Table of Contents

List of Contributors

A. Joint Working Group (JWG) Chairman:

Name	Designation	Organisation	E –mail Address
Mahabir Parshad Singhal	Sr.DDG	Telecommunication Engineering Centre (TEC)	srddg.tec@gov.in

B. Joint Working Group (JWG) Secretariat:

Name	Designation	Organisation	E –mail Address
Shailendra K Sharma	DDG	Telecommunication Engineering Centre (TEC)	ddgsn.dl.tec@gov.in
Ratna Thakur	DIR	Telecommunication Engineering Centre (TEC)	dirsn.tec@gov.in
Manish Ranjan	ADG	Telecommunication Engineering Centre (TEC)	adgi2.tec@gov.in

C. Sub- Group (SG) Chair//LPCC(Lead Person Coordination Committee):

Name	SG-Chair	Organisation	E –mail Address
Vikas Phogat	SG-I	Idemia	vikas.phogat@idemia.com
Sumit Monga	SG-II	Unlimit	sumit.monga@relianceada.com
Sharad Arora	SG-III	Sensorise Digital	sharad.arora@sensorise.net
Vijay Madan	SG-IV	TSDSI	vijay.madan@tsdsi.org
Aurindam Bhattacharya	SG-V	C-DOT	aurindam@cdot.in

D. Sub-Group Members:

i. Sub-Group-I (End Point Devices Security):

S/n	Name	Organisation
1.	Pranav Singh	Idemia
2.	Amit Gupta	Eron Energy
3.	N. Kishor Narang	Narnix Technolabs
4.	Sudhir Kamble	TCTS
5.	Mukesh Dhingra	TTSL
6.	Praveen Singh	Eron Energy
7.	Shailendra.K. Sharma	TEC
8.	Sanjeev Sharma	DOT

ii. Sub-Group-2 (Network Communications Security):

S/n	Name	Organisation
1.	Sumit Monga	Unlimit
2.	Debabrata Nayak	Huawei
3.	Vikas Phogat	SAFRAN
4.	N. Kishor Narang	Narnix Technolabs
5.	Dinesh C. Sharma	ETSI
6.	Ranjana Sivaram	TEC
7.	Madhav Chablani	CSA
8.	Divya Sharma	TEC
9.	Manish Ranjan	TEC

iii. Sub-Group-3 (Application Level Security):

S/n	Name	Organisation
1.	Sharad Arora	Sensorise
2.	Sudhir Kamble	TCTS
3.	Debabrata Nayak	Huawei
4.	Sumit Monga	Unlimit
5.	Dinesh Chand Sharma	ETSI
6.	Madhav Chablani	CSA
7.	Ratna Thakur	TEC
8.	Manish Ranjan	TEC

iv. Sub-Group-4 (Trusted Environment):

S/n	Name	Organisation
1.	Vijay Madan	TSDSI
2.	Sudhir Kamble	TCTS
3.	Debabrata Nayak	Huawei
4.	Mukesh Dhingra	TTSL
5.	Aurindam Bhattacharya	C-DOT
6.	Shailendra.K. Sharma	TEC
7.	V.K. Arya	Retired (TEC)

v. Sub-Group-5 (Service Layer):

S/n	Name	Organisation
1.	Aurindam Bhattacharya	C-DoT
2.	Madhav Chablani	CSA
3.	Dinesh Chandra Sharma	ETSI
4.	Sharad Arora	Sensorise
5.	Ratna Thakur	TEC
6.	Divya Sharma	TEC
7.	Rakesh Kumar	MTNL
8.	Manish Ranjan	TEC

E. Primary Authors:

Name	Organisation
Sharad Arora	Sensorise
Shailendra. K. Sharma	TEC

F. Editorial & Advisory Group:

S/n	Name	Organisation
1.	Vijay Madan, Chairman of SWG	TSDSI
2.	G. Narendra Nath	DoT
3.	Rajiv Sinha	DoT
4.	Aurindam Bhattacharya	C-DoT
5.	Sumit Monga	Unlimit
6.	Vikas Phogat	Idemia
7.	Pranav Singh	Idemia
8.	N. Kishor Narang	Narnix Technolabs

G. Contributors:

S/n	Name	Organisation
1.	Sharad Arora	Sensorise
2.	Vijay Madan	TSDSI
3.	Sumit Monga	Unlimit
4.	Aurindam Bhattacharya	C-DoT
5.	Vikas Phogat,	Idemia
6.	Pranav Singh	Idemia
7.	Dinesh C. Sharma	ETSI
8.	Amit Gupta	Eron Energy
9.	N. Kishor Narang	Narnix Technolabs
10.	Sudhir Kamble	TCTS

11.	Mukesh Dhingra	TTSL
12.	Praveen Singh	Eron Energy
13.	Shailendra.K. Sharma	TEC
14.	V. K. Arya	Retired (TEC)
15.	Madhav Chablani	CSL
16.	Ratna Thakur	TEC
17.	Manish Ranjan	TEC
18.	Divya Sharma	TEC

Table of Figures

1. Background and Scope

1.1. Background

M2M, the acronym for Machine-to-Machine communication is an emerging area in the field of telecom technologies. Machine to machine (M2M) refers to technologies that allow both wireless and wired systems to communicate with other devices of the same ability. M2M uses a device (such as a sensor or meter) to capture an event, which is relayed through a network (wireless, wired or hybrid) to an application, that translates the captured event into meaningful information.

ITU-T in its recommendations, ITU-T Y.2060 (06/2012) has defined Internet of things (IoT) as ***"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. Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled."*** ETSI has defined M2M Communications in ETSI TR 102 725 V1.1.1 (2013-06): as ***Physical telecommunication based interconnection for data exchange between two ETSI M2M compliant entities, like: device, gateways and network infrastructure.***

M2M Ecosystem comprises of telecom service providers, M2M application service providers, Sensors, hardware OEMs, supply chain, middleware, deployment and asset management. Varying requirement of mobility and dispersion level in different applications of M2M and Network Technology used can be explained as per the following diagram (Figure 1):

		NEED OF MOBILITY →	
		FIXED	**MOBILE**
GEOGRAPHICAL SPREAD →	DISPERSED	**Applications** Smart Grid, Smart Meters, Smart City Remote Monitoring **Technology** PSTN Broadband 2G/3G/4G Power Line Communication	**Applications** Car Automation eHealth Logistics Portable Consumer electronics **Technology** 2G/3G/4G Satellite
	CONCENTRATED	**Applications** Smart Home/ Smart Building Factory Automation eHealth **Technology** Wireless Personal Area Network Wired Network Indoor Electrical Wiring Wi-Fi	**Applications** On Site Logistics **Technology** Wi-Fi WPAN

Figure 1: Requirement of mobility and dispersion level in different applications of M2M and Network Technology.

M2M is driving an increasingly complex relationship between networks, service providers and an exploding number of devices in real time. These devices will be powered and connected by a complicated

convergence of networks. Different types of applications have different needs in terms of network resources leading to requirement of different regulatory treatment to them. DoT endeavours to tackle the regulatory implications of usage of digital communication technologies, including wireless, wire line, MPLS, Ethernet, Private Line, etc. in M2M applications.

The emergence of new service formats such as Machine-to-Machine (M2M) communications (e.g. remotely operated irrigation pumps, smart grid etc.) represent tremendous opportunities, especially as their roll-out becomes more widespread. To facilitate the role of new technologies in furthering public welfare and enhanced customer choices through affordable access and efficient service delivery, TEC has released the following technical reports regarding M2M in the past:

1. M2M Enablement in Power Sector
2. M2M Enablement in Intelligent Transport System
3. M2M Enablement in Remote Health Management
4. M2M Enablement in Safety & Surveillance Systems
5. M2M Gateway & Architecture.
6. M2M Number resource requirement and options
7. V2V / V2I Radio Communication and Embedded SIM
8. Spectrum requirements for PLC and Low Power RF Communications.
9. ICT Deployments and strategies for India's smart cities: A curtain raiser
10. M2M / IoT Enablement in Smart Homes
11. COMMUNICATION TECHNOLOGIES in M2M / IoT Domain

The TEC technical report on M2M Gateway and Architecture had highlighted the following general security requirements are applicable to M2M networks:

- **Availability**: Information network should be available for use of the concerned parties in the manner intended. This can be ensured by monitoring the network at device level, communication level and at the control center end.
- **Authentication**: This should provide assurance that a party in data communication is who or what they claim to be.
- **Authorization**: This security service should ensure that a party may only perform the actions that they are allowed to perform.
- **Integrity:** Integrity should ensure that data/ information cannot be altered in an unauthorized or malicious manner. Architecture should include strong Point to point communication schemes to prevent spoofing and injection of false data.
- **Confidentiality**: Data and information should be protected from being disclosed to third party. Confidentiality of data and information is achieved by providing role based access at both data & information level and at device level

1.2. Scope of the Workgroup

TEC, (Telecom Engineering Centre), the technical arm of DoT has started working on India specific M2M requirements / standards in line with evolving Global standards. With the above objective in mind various working groups have been formed in TEC and Security in M2M is one of them to facilitate communication standards for Security as well as privacy including encryption by incorporating in their technical reports / guidelines.

The scope of this version of the document is to create a common understanding and an aggregation of the recommendations submitted by the five sub groups of the M2M Security Work Group and enables the finalisation of the report for approval by the Senior DDG, TEC

The document presents a brief summary of the M2M Security Reports and Specifications and assimilates the views from the various documents circulated by the TEC Secretariat that are relevant to the working of the M2M Security Work Group.

The issues to be taken up/scope to be defined by various sub-groups include:

a. Incorporation of minimal security standards for M2M products and services with interoperability in view.

b. Define guidelines from security angle with respect to

- **Data ownership and retention period**
- **Security of sensitive data**
- **Location of application services**
- **Location of remote terminal unit/M2M devices**
- **Location of core n/w elements.**

c. Define policy/standards from security angle to connect legacy and non-IP devices on existing n/w technologies.

d. Define precautions/security conditions for voice/SMS/MMS/video on M2M.

e. Aspects to be taken care of with respect to security framework for various verticals and solutions.

f. Define separate KYC norms for M2M from security angle.

g. Requirement of M2M product certification from security point of view.

The activities that were carried out by this group included, in-depth and exhaustive discussions done over conference and face to face meeting on various aspects of security and on various standards /reports available globally. In the face to face (F2F) meeting in Feb 2017, security standards available i.e., oneM2M, GSMA,3GPP,ITU-T etc were presented and deliberated upon in detail and thereafter five sub groups were formed with Lead Person Cum coordinator as given below:

Sub-Group	LPCC (Lead Person Cum Co-ordinator)
Sub group 1 : End Point Devices Security	Sh. Vikas Phogat
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

The LPCCs had discussions within their own sub-groups as well as with other LPCCs in the various face to face meetings and through audio conference meetings for discussions and deliberations to prepare the draft document. Thereafter F2F meetings on 19-March 2018, 7th Sep 2018 and a Presentation on 21st August 2018 supported by various audio and web conferences in the months to follow, led to the making of this document on M2M security domain.

2. Notes from the Editorial Team

2.1 Editor's Note

A good Technical Standard / Report must be readable, not just for the evolved technocrat, but also for the common man who implements the standard in his business or work.

It must also be relevant to the context of the industry, and to the extent possible, to the existing policy and regulatory environment.

It must also bring guidance about inter-operability, especially in the context of M2M and IoT, where the industry is evolving with innovation from tens of thousands of start-ups and existing businesses worldwide.

2.2 Purpose

The purpose of this document is to make recommendations on the issues defined at 1.2, which may act as guidelines to the stakeholders in M2M after studying various standards available. M2M Security WG Recommendations are expected to act as a guideline in Policy Making that prompts the use of appropriate standards 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

2.3 Notes from the work group members

Aside from technical inputs, the subject of Internet of Things and Machine to Machine communications evokes all types of thoughts, philosophies, wisdom and advice. The section below presents these thoughts which are reproduced below as they assist in setting the context for this Technical Report.

- Identification, Authentication, Authorization and Trust mechanisms must be a fundamental part of every IoT / M2M service
- Test for Scale
- Verify data from the Edge
- Apply Data Protection [encryption] uniformly across all the legs and lifecycle stages of IoT Data
- Undertake a thorough review of key management and encryption to avoid common pitfalls
- Strip IoT Applications to minimum functionality to reduce the attack surface
- Limit access [to Applications / Device] to the minimum possible
- Transitive Ownership: Agile and capable Subscription lifecycle management is essential. Setup IoT applications to expect changes – e.g. Provisioning new sensors and services, removing old ones, Transferring Devices, reviewing and changing privileges etc.
- Prepare for complex N:N trust and authentication capabilities. The exponential increases of connected devices, use cases, applications would radically increase the need to collect, store, process personal and sensitive data.
- Security becomes a very important component of entire context aware ecosystem of platforms as well as clouds in which these machines, devices, services operate resulting in a physical, transactional or analytical outcome
- A Trust Environment providing security, privacy and accountability between all the stakeholders in the IoT ecosystem is a must
- Consider lightweight security protection methods
- Enhance device protection, such as by using the trusted platform module (TPM)
- Automation of threat detection and security measures is critical, use of a mature security analysis methods and protection technologies has to be mandated

- IoT / M2M service Providers must consider the privacy of their consumers and develop privacy management interfaces that are integrated into both the endpoint, and the product or service's web interface
- Each peer in an IoT ecosystem must authenticate all other peers that participate in that ecosystem
- Secure, over-the-air device management and remote provisioning of connectivity parameters must be mandated
- It is vital to have a mature policy, governance and regulatory framework for the ownership, use and transferability of the device, platforms and user data

3. Introduction to IoT / M2M

3.1 IoT / M2M Landscape

M2M (Machine to Machine communication) is an emerging area for connecting devices, M2M refers to technologies that allow both wireless and wired systems to communicate with other devices of the same ability. M2M uses a device (such as a sensor or meter) to capture an event, which is relayed through a network (wireless, wired or hybrid) to an application, that translates the captured event into meaningful information. We foresee a heterogeneous architecture in future, in which there will be several devices, gateway and back end platforms will be communicating to each other using different communication modes.

Internet of Things: 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.

This report defines Security for IoT as follows

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

The official website of Department of Telecommunications says the following regarding M2M/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. It may be applied to robots and conveyor belts on the factory floor, to tractors and irrigation on the farm, from heavy equipment to hand drills, from jet engines to bus fleets; from home appliances to health monitoring; from Smart Grid to Smart Water; every piece of equipment, everywhere. It can bring substantial tangible social and economic benefits by giving more efficient and effective services to the citizens."

Wikipedia defined "The Internet of Things" as "the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to connect and exchange data". According to Jacob Morgan of Forbes, "this is the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other). This includes everything from cell phones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of. This also applies to components of machines, for example a jet engine of an airplane or the drill of an oil rig. As I mentioned, if it has an on and off switch then chances are it can be a part of the IoT. The analyst firm Gartner says that by 2020 there will be over 26 billion connected devices. That's a lot of connections (some even estimate this number to be much higher, over 100 billion). The IoT is a giant network of connected "things" (which also includes people). The relationship will be between people-people, people-things, and things-things".

While the rapid growth of the Internet of Things represents a major opportunity for all members of the new ecosystem to expand their service offerings and increasing their customer base, analysts have indicated that security issues are a significant inhibitor to the deployment of many new IoT services. There is already much evidence to show that attackers are beginning to show ever greater interest in this area.

As these new service providers develop new and innovative services for particular market segments, they may be unaware of the threats their service may face. In some cases, the service provider may not have developed a service that has connected to a communications network or the internet before and they may not have access to the skills and expertise to mitigate the risks posed by enabling internet connectivity within

their devices. In contrast, their adversaries understand the technology and security weaknesses, quickly taking advantage if vulnerabilities are exposed.

Whilst many service providers, such as those in automotive, healthcare, consumer electronics and municipal services, may see their particular security requirements as being unique to their market, this is generally not the case. Almost all IoT services are built using endpoint device and service platform components that contain similar technologies to many other communications, computing and IT solutions. In addition to this, the threats these different services face, and the potential solutions to mitigate these threats, are usually very similar, even if the attacker's motivation and the impact of successful security breaches may vary.

In view of this, it is imperative to analyse the role of security in M2M and prepare a set of recommendations which may act as a guideline to all the stakeholders.

M2M infrastructure consists of measurement devices, gateway devices/ aggregators, communication network for information exchange and control centre to collect data & information and use it for the intended operations. Information is exchanged at device level where it is generated, during exchange on the communication network and at control centre where it is collected for intended use.

The architecture will include measures to ensure security of data at different modes like security for systems, communications and also service provider/operations.

Security is one of the most important considerations while designing an M2M system, in order to prevent the hackers to break into M2M applications designed to control, for example, building security, environmental monitoring, vehicle tracking, etc. In order to prevent possible security violations, the most appropriate communication techniques must be used, because different types of communication techniques present different encryption and security features.

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, not excluding capabilities that may be provided by third parties such as data analytics.

IoT Sustainability: Defined as sustainability, it is the mitigation of the risk and implications of having devices, systems, nodes, back and front ends and platforms that are left un-patched, orphaned, or bricked, which is critical to realizing the promise of IoT. Sustainability also includes the policy, governance and regulatory issues related to the ownership and transferability of the device, platforms and user data. Since devices may outlive an owner or be transferred to new home buyers, consumers and businesses need the assurance that companies will continue to address these needs after the expiration of their traditional warranty.

Each peer in an IoT ecosystem must authenticate all other peers that participate in that ecosystem. To accomplish this, a given player's process must be used to ensure that proper cryptographic architecture is driving the communications technology. Mutual authentication can't occur if keys are easily exposed to adversaries.

Once authenticated, each peer must encrypt and sign messages sent to other peers in the network. Each peer that receives a message must cryptographically validate the data prior to acting on it.

Since not all communications protocols are capable of mutual authentication, or have strong cryptography, it is imperative that the application entities in the value chain design a sufficient protocol that enforces confidentiality and integrity, rather than relying on the communications protocol. Even more robust protocols that incorporate mutual authentication, such as LTE, do not address the security of the infrastructure beyond the cellular communications network. Only higher layer protocol security can address the risk of weaknesses in infrastructure beyond the control of the cellular carrier.

It is important that IoT / M2M service Providers consider the privacy of their consumers and develop privacy management interfaces that are integrated into both the endpoint, where possible, and the product or service's web interface. This technology should allow the user to determine what attributes of their privacy are being utilized by the system, what the terms of service are, and the ability to turn off the exposure of this information to the business or its partners.

Each Endpoint is known digitally by a fingerprint. This fingerprint is composed of addresses, serial numbers, and cryptographic identities that are unique to the specific Endpoint. Security of End Point Applications: Applications running on an endpoint typically do not require super-user privileges. Most often, applications require access to device drivers or a network port. While, some of these devices, ports, or other objects may require super-user privileges to initially access them, the super-user privileges are not required to perform subsequent operations. Thus, it is best practice to only use super-user privileges at the start of the application to gain access to these resources.

Device Management: The underlying principle of M2M communications isn't particularly new, as similar technology has been used for decades at power stations, water utilities, building control and management systems, and the like, usually in the more recognisable form of supervisory control and data acquisition (SCADA) systems. However, these systems are typically custom implementations, often running proprietary operating systems, and without any particular standard to follow. They weren't designed with security in mind when they were designed. The designer did not expect them to necessarily be connected to the internet [or] a public access network. They probably more anticipated that they would be behind a secure network, and they made some assumptions on how it works. But nowadays most of the devices are on internet. They talk IP, and they have massively vulnerable operating systems.

IoT cloud: The idea of the local cloud is to have all things that are required for M2M/IoT environment. This can include many nodes, micro-controllers, embedded devices, smart meters, sensors and actors. The policies are required when the user want to share the data within the local cloud with other users or to send it to the Internet. The communication between different clouds must be secured and the users must have trust in the destination cloud which will process their data. This can happen with the help of certificates directly between parties.

Identification, Authentication, Authorization and Trust:

Identification of objects / things is a prerequisite for the safety and security of IOT ecosystem. ITU in its document ITU-T F.748.1 has come out with the recommendation to identify things / objects both physical as well as virtual, highlighting the common characteristics in the IOT Identifier and the Requirements of IOT Identifier along with mapping of IOT Identifier to objects. In India GSM connectivity Identifier (MSISDN) for M2M use cases has been changed from 10 to 13 digits.

Authentication mechanisms should work side-by-side with distributed trust management and verification mechanisms. Most common method for authentication is to provide username and password. Another method for authentication is SSO (Single Sign-on), which help to reduced sign-on and avoid continually re-authenticating for each application. (Example: Home Cloud of an Enterprise). At the heart of this framework is the authentication layer, used to provide and verify the identify information of an IoT entity. When connected IoT/M2M devices (e.g., embedded sensors and actuators or endpoints) need access to the IoT infrastructure, the trust relationship is initiated based on the identity of the device. For example, in typical enterprise networks, the endpoints may be identified by a human credential (e.g., username and password, token or biometrics).

Authorisation: The second layer of this framework is authorization that controls a device's access throughout the network fabric. Network enforced security policy layer encompasses all elements that route and transport endpoint traffic securely over the infrastructure, whether control, management or actual data traffic. Like the Authorization layer, there are already established protocols and mechanisms to secure the network infrastructure and affect policy that are well suited to the IoT/M2M use cases. This layer

encompasses all elements that route and transport endpoint traffic securely over the infrastructure, whether control, management or actual data traffic.

Trust: Each organization must individually certify that every other participating organization is worthy of its trust. The issue with cross-certification trust model is that when the number of participating cloud grows, the numbers of trust relationships grows also. For example, a car may establish a trust alliance with another car from the same vendor. That trust relationship, however, may only allow cars to exchange their safety capabilities. When a trusted alliance is established between the same car and its dealer's network, the car may be allowed to share additional information such as its odometer reading, last maintenance record, etc.

This document gives the basic summary of the role of security in M2M. It evaluates the threats and challenges and recommends potential solutions after the study of various relevant standards.

The study has been divided broadly into 5 main parts namely, (i) Endpoint devices security, (ii) Network communication security, (iii) Application level security, (iv) Trusted Environment and (v) Service layer security.

The document has identified the issues and challenges of security in M2M in the light of various standards available i.e. One M2M, GSMA, 3GPP, ETSI etc., which were presented and deliberated upon in detail in various working group meetings.

The security analysis of the general M2M Network Architecture and the deployment models considering oneM2M security framework has to be further studied in detail.

3.2 How is IoT different from M2M?

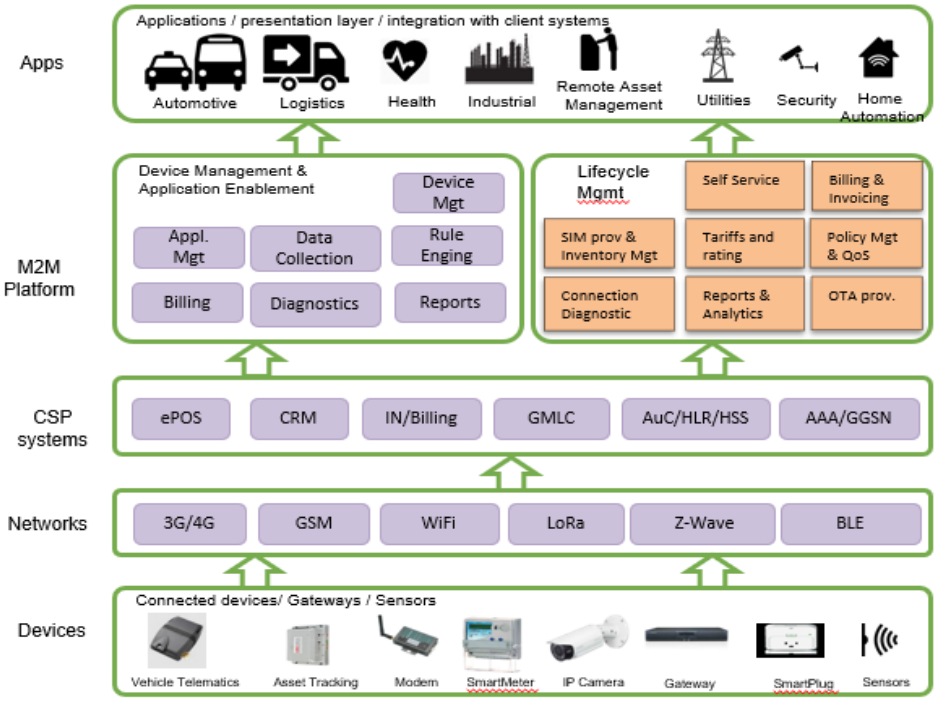
A question that often crosses the mind of a lay user and is equally often ignored is – what is the difference between M2M and IoT. The diagram below (Figure 2) addresses this matter in a simple comparison of the two terms.

What	M2M	IoT
Genre	SCADA and Industrial Automation	New Age Solutions
Connectivity	Point to Point Connectivity	IP based Connectivity
Motivation	Remote access to machines	Remote access to everything
Networks	Wired or Cellular	All types of wired / wireless Networks
Applications	For Industrial Machines / Data	For Individuals, Things, Enterprises
Beneficiary	Mostly Single User / Entity	Multi-user / Mass benefits
Solution focus	Embedded, Comms Modules	Enterprise integration, Big Data, Apps
Analytics	Machine / Industry Performance	Big Data analytics for smart cities, health, sentiments, vehicles, infra

Figure 2: Difference between IoT and M2M

3.3 IoT Solution Landscape

The info graphics below (Figure 3) shows one possible view of the IoT Solution landscape.



View of IoT Solution Landscape

Figure 3: IoT Solution Landscape

The BIS Pre-standardisation Report titled 'Requirement Analysis of Unified, Secure and Resilient ICT Framework for Smart Infrastructure, November 2017, Ver 1.0' pictures the solution domain as below (Figure 4)

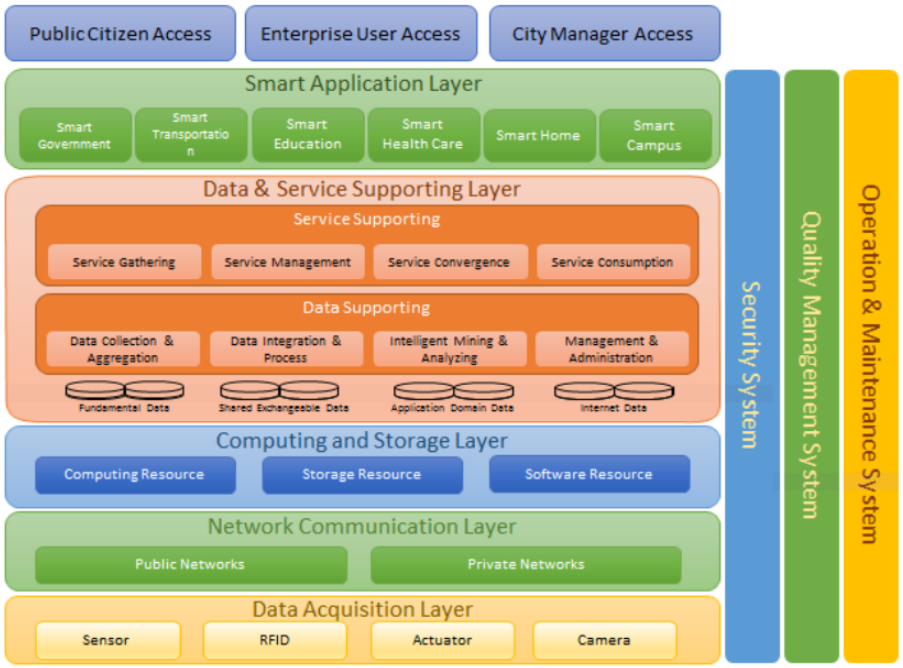


Figure 4: BIS Smart City ICT Framework

3.4 Functional Architecture and Domains

The Report examines the IoT / M2M ecosystem in functional domains as shown below (Fig 5):

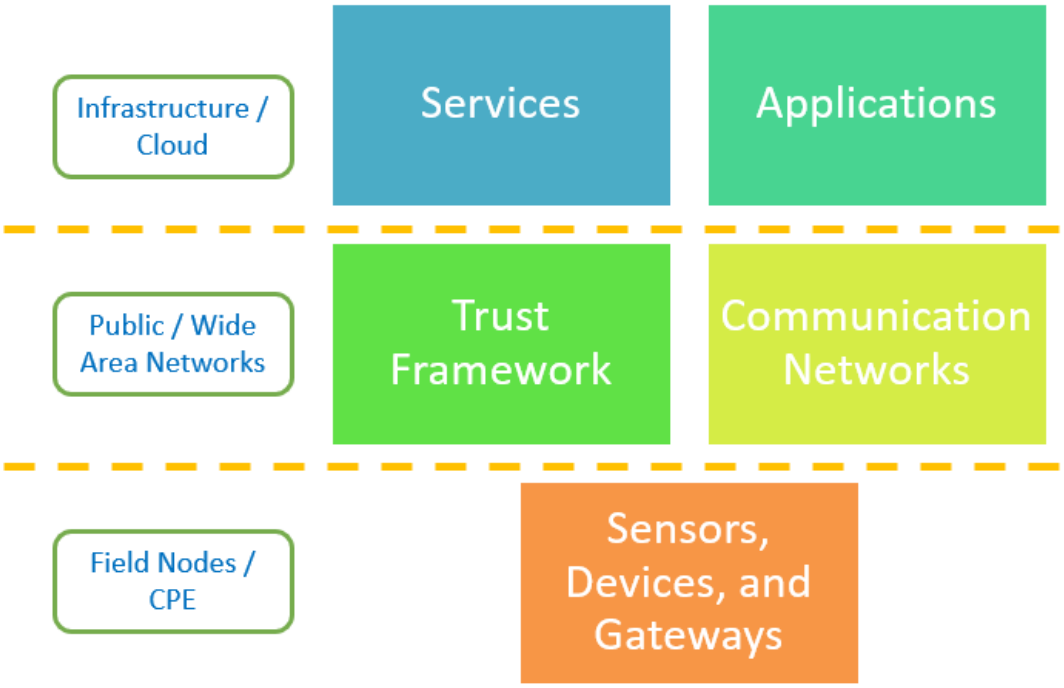


Figure 5: Functional View

This report addresses the security aspects in the five domains described above. The IoT / M2M solution can also be appreciated from a geographical lens. Sensors, Devices and Gateways are usually the dispersed nodes, found in the field and customer premises. Networks vary in scale from small areas and neighbourhoods to cities, states and country wide networks. Applications and Services are mostly delivered from Data Centres and Clouds, centralised in a few places. Trust frameworks are all pervasive; these are embedded into Field Nodes, Communication Networks, Applications and Services.

M2M / IoT is a widely researched field today, and several reference frameworks exist from various standardisation and industry bodies. A few important examples of M2M frameworks are provided below as illustrative references, these are not intended for the purpose of specification.

3.5 Example of ETSI M2M Architecture

The ETSI M2M Architecture addresses the domains of M2M Device and Gateway on one side, and the M2M Network Domain on the other side. ETSI M2M has adopted a RESTful architecture where information is represented by resources which are structured as a tree. ETSI M2M standardizes the resource structure that resides on an M2M Service Capability Layer (SCL). Each SCL contains a resource structure where the information is kept. The M2M Application and/or M2M Service Capability Layer exchange information by means of these resources over the defined reference points. ETSI M2M standardizes the procedure for handling the resources.

The ETSI M2M Architecture is summarised below (Fig 6)

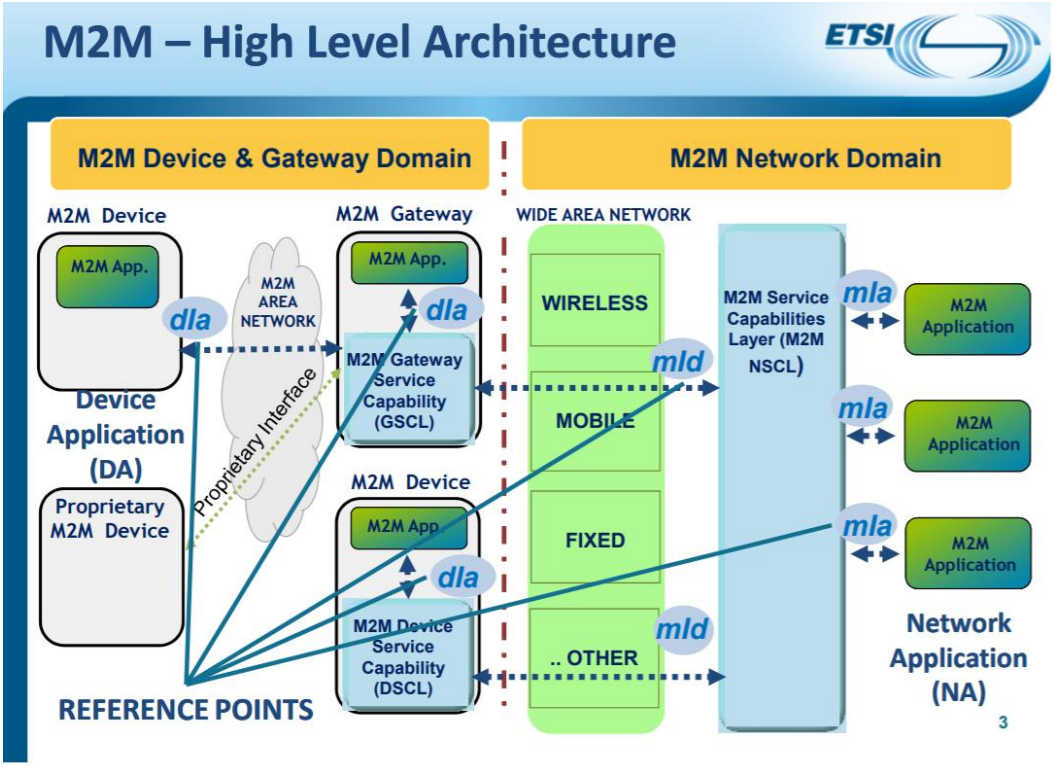


Figure 6: ETSI M2M Architecture, Barbara Pareglio, Ericsson

The ETSI M2M Architecture relies on the following important concepts

- Identification of the M2M Application and the M2M Devices.
- Asynchronous and synchronous communication
- Store and forward mechanism based on policies for optimising the communication
- Location information
- Device management based both on OMA DM (wireless) and BBF TR-69 (wireline)
- Mutual authentication between Network Service Capability Layer and Device/Gateway Service Capability Layer that are connected
- Secure channel for transporting data over mId reference point
- The device/gateway needs to have keys for securing the connection. The device/gateway is provisioned with the key M2M Root Key. The high-level procedure requires mutual mId end point authentication, M2M Connection Key agreement, or establishment of a secure session over mId
- RESTful procedures over the mId
- The Network Application registers to the NSCL [Trust Registry], the gateway registration results in a resource representation in the GSCL

3.6 Example of GSMA IoT Model

The primary components of IoT can be explained with Figure 7 showing components of GSMA IoT model, i.e. End Point Devices (consisting of low complexity devices, rich/complex endpoint devices and gateways that connect the physical world to the digital world), Service Ecosystem (the set of services, platforms, protocols, and other technologies required to provide capabilities and collect data from Endpoints deployed in the field) and Communications network components providing the connection between the two ecosystems.

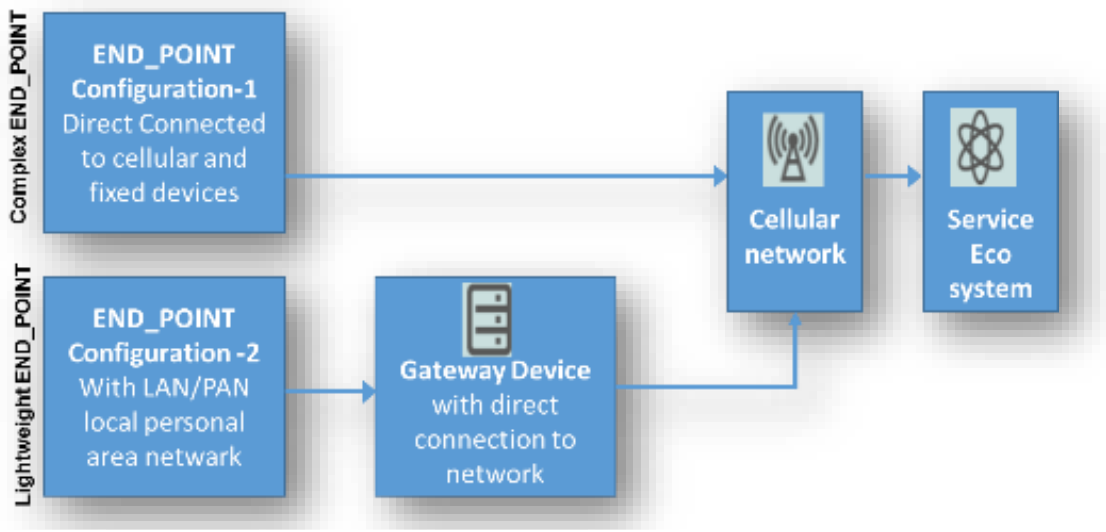


Figure 7: GSMA Security Model

3.7 Global Platform Security Model

The Figure 8 below describes the Global Platform Security Model.

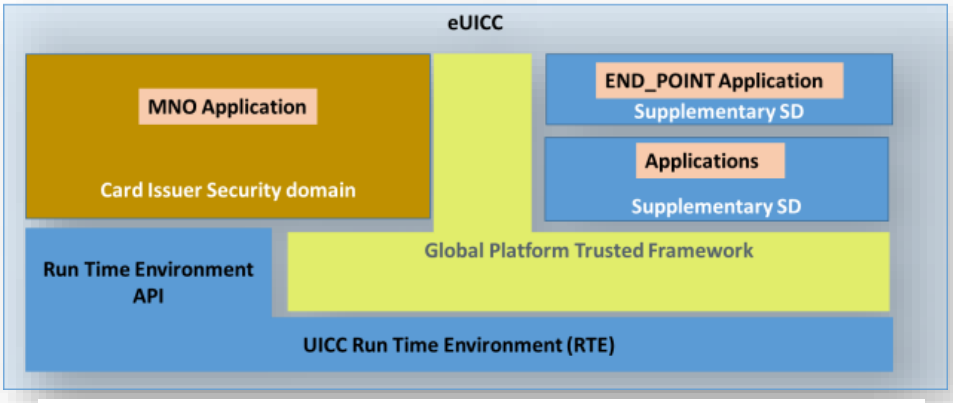


Figure 8: Global Platform Security Model

An important feature of a Global Platform enabled eUICC card is its ability to support multiple isolated and independent security domains. Through this feature, END_POINT service providers can independently store and administer their own security credentials within the eUICC, which can then be used by other components within the END_POINT system.

3.8 Example of OneM2M Reference Architecture

To understand the framework of IoT, we can look at the reference architecture in Figure 9 by OneM2M. OneM2M, one of the emerging global standards in the area of M2M/IoT, has identified four security domains. Each of these domains provides security features to meet certain threats and in particular protect against attacks, in associated trust scenarios.

(1) Application domain security: the set of security features that enable Applications and Common Services to securely exchange messages and protect against attacks on the Mca Reference Points.

(2) Intra Common Services domain security: the set of security features that enable Common Service Functions in the Common Service Entity to securely exchange messages and which in particular protect against attacks on the CSE.

(3) Inter Common Services domain security: the set of security features that enable secure exchange of messages between CSEs and protect against attacks on the Mcc Reference Points.

(4) Underlying Network security: the set of security features that enable Underlying Network Services and Common Services to securely exchange messages and protect against attacks on the Mcn Reference Points.

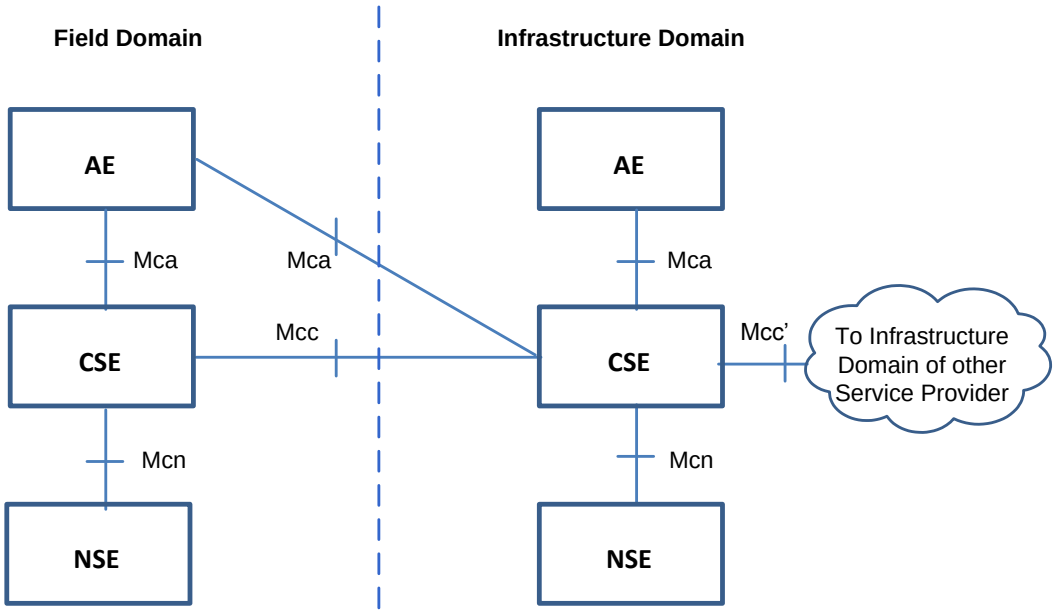


Figure 9: One M2M functional architecture

The oneM2M architecture defines the security framework for building more intelligent and autonomous M2M system. It attempts to resolve the security issues in communication and control problems between machines with difference in technical characteristics that make them part of the global Internet network. The secure software framework allows systems to function in different application domain. Providing reliable services is complicated by the fact that different parts of the network are provided by different entities. The security analysis of the general M2M Network Architecture and the deployment models considering oneM2M security framework has to be further studied in detail.

Figure 10 depicts the oneM2M Layered Model for supporting the end-to-end (E2E) Services. This layered model comprises three layers. Application Layer, Common Services Layer and the underlying Network Services Layer.

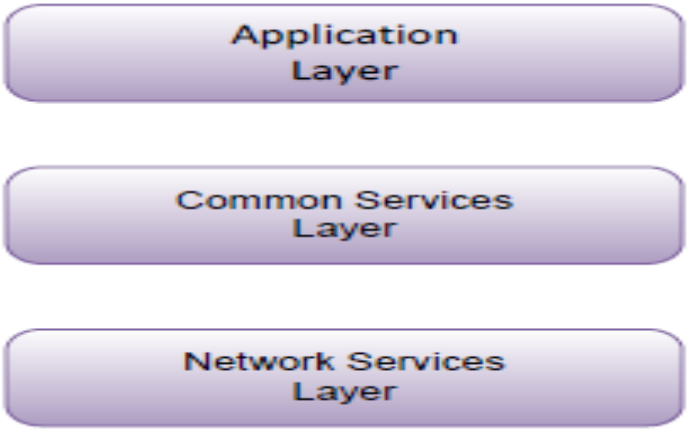


Figure 10: OneM2M Layered Model

3.8.1 One M2M Applications

As per the OneM2M Security Architecture, an M2M Application Service Provider can rely on independent credentials to secure its End-to-End communications, so that application related information is not exposed to either the M2M Service Provider or the underlying network operator. The M2M System provides an interoperable interface for provisioning and administration of security credentials in M2M nodes which can be used by the M2M Application or any trusted third party that is involved in application security.

3.8.2 OneM2M Common Services

In cases where the M2M Service provider is entrusted to provide security to the M2M Application, the ability to secure communication between nodes for the purpose of the M2M Service Layer can be made directly available by M2M Service Providers to the M2M Applications through an API.

3.8.3 OneM2M Underlying Network

In cases where the underlying network provides secure communication for M2M Equipment that is trusted by the M2M Application Service Provider, the key derivation and secure connection establishment capabilities exposed by the underlying network can be used by the M2M System in the infrastructure domain, based on long term keys provided by the underlying network. There is a need for the M2M System to extend the provisioning of such security to edge nodes that are not directly connected to the underlying network (e.g. because they are behind a gateway).

3.8.4 OneM2M Trust Provider

The Application Level Security must ensure that AEs distributed across domains, Nodes and M2M SPs can interact with each other without compromising security.

To fulfil this requirement, it must provide for the following

- Trust Provider Requirements when the M2M SP is the Trust Provider
- Trust Provider Requirements when a Trusted Third Party is the Trust Provider
- Recommendations for the Registration procedures for the M2M SPs, AEs and CSEs, as also the requirements for mutual authentication
- M2M Authorization functions for authorization of requests to access resources across M2M SPs, Domains and Layers

4 Setting the Policy and Regulation context

4.1 Proactive Policy and Regulation

The Government of India, through several ministries and ministerial groups, has made M2M/IoT a national agenda. The Departments of Telecommunications has released a National Telecom M2M Roadmap as far back as May 2015. The New Technologies cell of the DoT is engaged in formulation of KYC Norms for SIM embedded M2M Devices, Numbering scheme for M2M, Registration of MSP (M2M Service Provider) and M2M Pilots. DoT has sought from TRAI its recommendations on Roaming issues, Spectrum Requirement and Quality of Service (QoS) in M2M communications. Consequently, TRAI released its consultation paper titled 'Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications' in October 2016. TRAI released its recommendations on 'Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications' on 5th September, 2017 (available on its website www.trai.gov.in). The Telecom Act has recently been amended to require Certification of all M2M objects that connect to a public network, through a Gazette Notification as per reference in this document [17]. DoT has also released a policy for M2M KYC and e-SIM in May 2017, as per reference in this document [18].

4.2 National M2M Roadmap

The National M2M Roadmap highlight matters relevant to this report are as per Annexure - A

4.3 M2M Service Provider Registration

Developing identity and trust frameworks to deliver quality, secure and sustainable services is a vital requirement for proliferation of IoT / M2M Services. The few relevant sections of the Draft M2M Service Providers (M2MSP) Registration Guidelines released by the DoT on 14th Jun 2016 are as per Annexure - B

4.4 TRAI Guidelines

The honourable TRAI has conducted a nine-month long consultation on "Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications" releasing its recommendations on 5th September, 2017 [http://www.trai.gov.in/notifications/press-release/trai-releases-recommendations-spectrum-roaming-and-qos-related]. Relevant extract of TRAI's recommendations are as per Annexure – C.

4.5 M2M SIMs / e-SIMs

DoT has issued instructions on 16th May 2018 on M2M SIMs / e-SIMs and the related restrictive practices for bulk issuance and Know Your Customer norms. The Key highlights of the policy are as per Annexure - D

- TSPs shall issue M2M SIMs to M2M Service Provider as per the Bulk connection issuance policy
- The M2M SIMs shall have restrictions for Voice Calls to/from ONLY one predefined number, SMS to/from maximum of two predefined numbers, and Data to two predefined IPs
- Voice Calls to Emergency Numbers (Police, Fire, etc) shall not be restricted
- Ownership of all such M2M SIMs issued by the TSP shall be with the M2M Service Provider
- The User of the M2M Machine, Device and Connection [Custodian] shall be verified by the M2M Service Provider as per the norms and published online. In case of a change or transfer of the User, M2M Service Provider will undertake a fresh Custodian Verification and update the records in its database
- The e-SIM shall be allowed in single or multi profile, with over the air remote management
- In order to avoid TSP lock-in, TSPs shall facilitate profile updating Over-The-Air for all use case scenarios of e-SIM
- The TSP must ensure the Lawful Intercept and Monitoring of the M2M SIM

4.6 TEC Technical Reports

In line with the focus and thrust within the government, the Telecom Engineering Centre has published eleven technical reports for the IoT / M2M industry. Coordinated by TEC by inviting consultation from industry experts over several years, the M2M TEC reports offer the Industry critical insights and guidance in the IoT / M2M domains. These are listed below:

- M2M Gateway & Architecture
- M2M Enablement in Power Sector
- M2M Enablement in Automotive (Intelligent Transport System) Sector
- M2M Enablement in Remote Health Management
- M2M Enablement in Safety & Surveillance Systems
- M2M Number resource requirement & options
- V2V / V2I Radio communication and Embedded SIM
- Spectrum requirements for PLC and Low power RF communications
- ICT deployment and strategies for India's Smart Cities: A Curtain Raiser
- M2M/ IoT Enablement in Smart Homes
- Communication Technologies in M2M / IoT Domain

4.7 References to relevant BIS / Sector specific standards

Aside from the DoT, TEC and TRAI, IoT / M2M has become a national agenda with several stakeholders. Various agencies are involved in standardisation efforts, some relevant and important ones are noted below:

- AIS 140 Standard of Ministry of Road Transport and Highways
- BIS Standards and Technical Reports, including the Pre-standardisation Report titled 'Requirement Analysis of Unified, Secure and Resilient ICT Framework for Smart Infrastructure, November 2017, Ver 1.0'
- BIS standard IS 16833:2018 on Automotive Tracking Device and Integrated Systems (July, 2018)
- Ministry of Electronics and IT: Standards and Policies for Smart Cities and Infra
- Ministry of Power Smart Grid Guidelines and Policies

4.8 GSMA Guidelines, ETSI Standards & ITU Reports

The following documents are relevant to this Technical Report:

- GSMA IoT Security Guidelines Overview Document-2016
- ETSI M2M Architecture and ETSI TS 102 921:
- SIM Alliance Profile interoperability technical specification_V2.1 Final
- ETSI Specifications M2M UICC - TS102.671
- ITU-T F.748.1 on IOT Identifier Requirements

5. Security Threats, Challenges, Risks and Mitigation for Securing the IOT/M2M Ecosystem

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.

This section discusses the security threats and challenges for the IoT/M2M domain, their assessment and mitigation methods.

5.1 IoT/M2M Security Threats

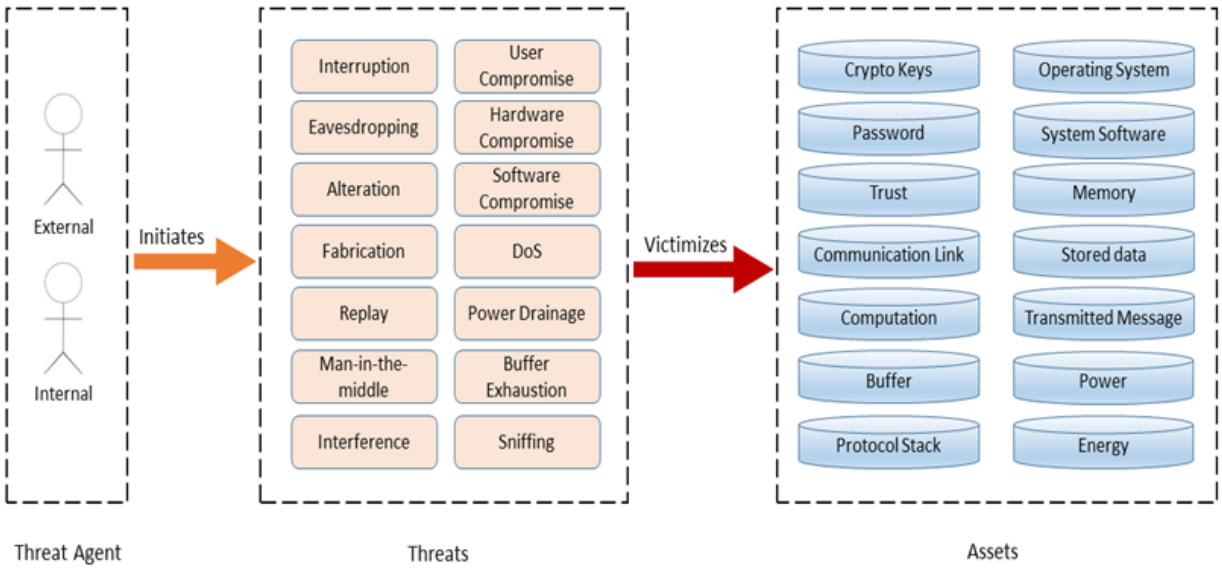
The Following stakeholders are affected by the IoT/M2M Security threats

- M2M Application Service Provider;
- Manufacturer of M2M Devices and/or M2M Gateways;
- M2M Device/Gateway Management entities;
- M2M Service Provider;
- Network Operator
- User/Consumer

5.2 Understanding the potential threats in IoT/M2M environment

In a completely closed network, like in a verticalized captive use case, security risks are minimal. But, as M2M embedded systems become IP-enabled and interconnected the attack surface becomes open to threats. Services provided by the IOT/M2M System to IOT/M2M applications establish the need for trusted security credentials to secure connections between applicative entities, including the other involved functions. IoT security requires a nuanced understanding of its unique characteristics.

An understanding of the potential threats in the IoT environment has been broadly shown in the (Figure 11) diagram as below, whereby various internal/external threat agents initiating threat by virtue of interruption, eavesdropping, buffer exhaustion, software/hardware compromise etc. which victimizes the various assets (like memory, crypto keys, buffer, power, energy etc.) and may cause malfunctioning of these assets.



Source: http://secret.cis.uab.edu/research/iot-security/

Figure 11: Potential threats in IoT

IoT opens a completely new dimension to security. The IoT is where the Internet meets the physical world. This has some serious implications on security as the attack threat moves from manipulating information to controlling actuation (in other words, moving from the digital to the physical world). Consequently, it drastically expands the attack surface from known threats and known devices, to additional security threats of new devices, protocols, and workflows. Many operational systems are moving from closed systems into IP based systems which further expands the attack surface.

For the most part, machines are unattended devices. People hesitate in adding security features like proactive monitoring as this could slow down performance and therefore at times the designers may have ignored security issues, in turn leaving devices vulnerable. The same also applies to embedded systems as CPU, battery life and memory all take priority and design choices are often made that favour speed of roll out over security. The inclusion of security component, such as cryptography, can slow communications and performance, impact and eat into processing capability of the device working on a very low power long term battery to sustain or survive.

In addition to the unique risks for IOT/M2M systems, embedded systems in general contain inherent security challenges as a number of pathways exist for threats to enter the system. M2M communication for embedded systems is straight-forward: embedded systems with microchips and wireless sensors reside at the bottom of a computer stack. These embedded systems communicate with each other via smart software applications and distributed computing systems. While distributed computing systems may allow for aggregation and increased communication speed, they also increase opportunities for attack. The smart software applications may have centralized servers that can be accessible to the internet.

While distributed computing systems (residing all through the nodes / systems including the end devices) may allow for aggregation and increased communication speed, they also increase opportunities for attack:

- The smart software applications may have centralized servers that can be accessible to the internet, causing an increase in attack.
- The distributed computers may have wireless access through which they can interact with either the smart applications or the sensors behind them, leading in an increased vulnerability.
- The sensors themselves may have physical connections that can be compromised.
- Threats also come from software libraries (inherited or custom), operating systems and packages, third-party communications and application porting from the cell or Wi-Fi ecosystem.

While IOT/M2M endpoints and IOT/M2M Gateways might be dedicated to specific IOT/M2M Services, IOT/M2M Systems as a whole will frequently share resources with a variety of other un-related systems and applications.

The devices and the control platform on which data may be consumed and shared could have different ownership, policy, managerial and connectivity domains. Consequently, devices will be required to have equal and open access to a number of data consumers and controllers concurrently, while still retaining privacy and exclusivity of data where that is required between those consumers.

Ensuring Information availability, while providing data isolation between common customers is critical. We must establish the appropriate identity controls and build trust relationships between entities to share the right information.

There are seemingly competing, complex security requirements to be deployed on a platform with potentially limited resources, which are enumerated below:

i. Authenticate to multiple networks securely
ii. Ensure that data is available to multiple collectors
iii. Manage the contention between that data access
iv. Manage privacy concerns between multiple consumers
v. Provide strong authentication and data protection (integrity and confidentiality) that are not easily compromised
vi. Maintain availability of the data or the service

vii. Allow for evolution in the face of unknown risks

These issues have particular relevance in the IoT where secure availability of data is of paramount importance. For example, a critical industrial process may rely on accurate and timely temperature measurement. If that endpoint is undergoing a Denial of Service (DoS) attack, the process collection agent must somehow be made aware. In such an event, the system should be able take appropriate actions in real-time, such as sourcing data from a secondary connection, or delay the information transmission. It must also be able to distinguish between loss of data due to an ongoing DoS attack and loss of the device due to a catastrophic event in the plant. It might accomplish this by using learning machine techniques (for example, comparing a normal operational state to an attack state previously learned).

IPv6, a foundation of the IoT, is subject to the same attack threats as IPv4, such as smurfing, reconnaissance, spoofing, fragmentation attacks, sniffing, neighbour discovery attacks, rogue devices, man in the middle attacks, and others. The IoT can be affected by various categories of security threats including the following:

i. Common worms jumping from ICT to IoT
ii. "Script kiddies" or others targeting residential IoT – Home control
iii. Organized crime: Access to intellectual property, sabotage, and espionage
iv. Cyber terrorism

Although the threats in the IoT environment might be similar to those in the traditional IT environments, the overall impact could be significantly different. That is why there are several efforts in the community to focus on threat analysis and risk assessments to gauge the impact if a security incident or a breach occurs. One of the fundamental elements in securing an IoT infrastructure is around device identity and mechanisms to authenticate it.

As mentioned earlier, many IOT devices may not have the required compute power, memory or storage to support the current authentication protocols. While the protocols are robust, they require high compute platform - a resource that may not exist in all IoT attached devices. Consequently, authentication and authorization will require appropriate reengineering to accommodate our new IoT connected world.

Secondly, these authentication and authorization protocols also require a degree of user intervention in terms of configuration and provisioning. However, many IoT devices will have limited access, thus requiring initial configuration to be protected from tampering, theft and other forms of compromise throughout its usable life, which in many cases could be years. In order to overcome these issues, new authentication schemes that can be built using the experience of today's strong encryption/authentication algorithms are required. The good news is that new technologies and algorithms are being worked on.

Other elements in security that could be considered include the following:

i. Application of geographic location and privacy levels to data
ii. Strong identities
iii. Strengthening of other network centric methods such as the Domain Name System (DNS) with DNSSEC and the DHCP to prevent attacks
iv. Adoption of other protocols that are more tolerant to delay or transient connectivity (such as Delay Tolerant Networks)

Issue of life time of encryption: For example, a power meter in a home may last fifty years, whereas the encryption protocol might survive half of that time before it is compromised. Lastly, the communication and the data transport channels should be secured to allow devices to send and collect data to and from the agents and the data collection systems.

5.3 Frauds and attacks in IOT/M2M systems

Most commonly, an attacker installs unauthorized IOT/M2M service-layer software and/or modifies authorized software functions in IOT/M2M Devices or IOT/M2M Gateways. This attack may be used to:

i. commit fraud, e.g. by the incorrect reporting of energy consumption;
ii. cause a breach of privacy by obtaining and reporting confidential information to the attacker
iii. cause the disclosure of sensitive data such as cryptographic keys or other credentials
iv. prevent operation of the affected IOT/M2M Devices/Gateways

The IoT/M2M ecosystem has many stakeholders which have an interdependency which may lead to a cascading effect - IOT/M2M Application Service Provider; Manufacturer of IOT/M2M Devices and/or IOT/M2M Gateways; IOT/M2M Device/Gateway Management entities; M2M Service Provider; Network Operator; User/Consumer.

5.4 Challenges in IoT/M2M Security

IoT security challenges can broadly be depicted by the Figure 12 below showing security challenges in various aspects of IoT such as authentication, confidentiality, privacy, access control etc.

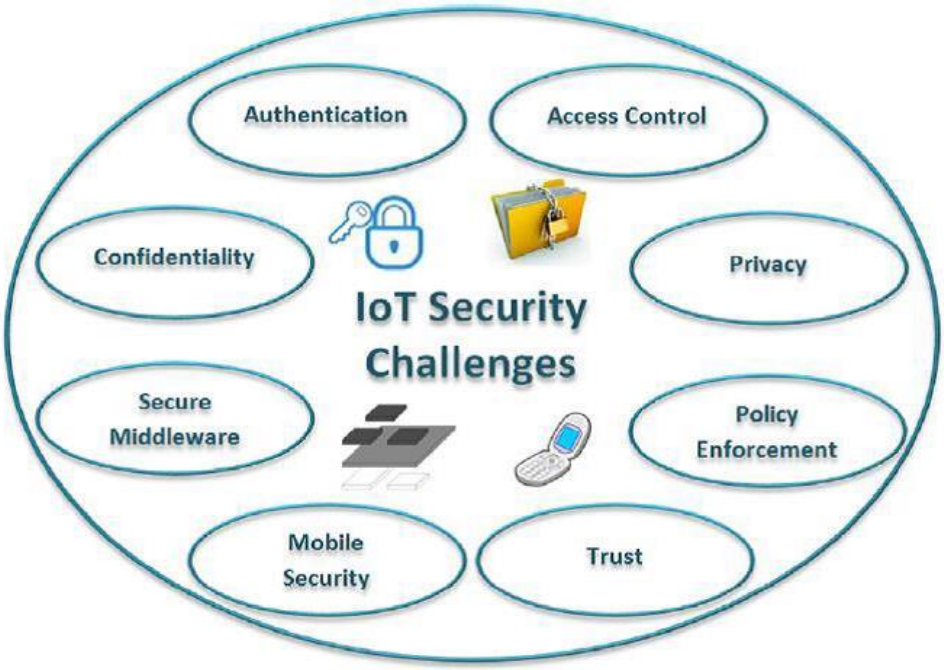


Figure 12: IoT Security Challenges (Source: Semantics Scholar.org)

5.5 Challenges - Security of Embedded Systems

In addition to the unique risks for M2M systems, embedded systems in general contain inherent security risks. These include: Firmware: The majority of software running on embedded systems is firmware, which can be easily changed, maliciously altered and then uploaded—replacing the authentic file. This may require external hardware or protocol reversal to achieve the objective, alternately, it can also be done with some reverse engineering. Otherwise, given physical access to the device, it is fairly easy to understand what the firmware is doing and to identify vulnerabilities within it.

Anti-tampering techniques when creating the firmware and the use of application whitelisting on devices in the field protect firmware from exploitation.

Many of the embedded systems in place today are unlikely to be connected to a network 100 percent of the time. Inconsistent or intermittent network connectivity increases the chances of a device connecting to an unsecured network. If an embedded system is online only occasionally, it is more likely to be dependent on a single node for network access, which creates a single point of failure or attack. Additionally, devices with

only occasional connectivity are more difficult to monitor for issues and more difficult to troubleshoot and upgrade.

In some cases, physical access to embedded devices is necessary for maintenance and upgrades. However, embedded devices that require or are open to physical access are exposed to two security threats.

i. First, it is more difficult to keep these systems up-to-date because they require human intervention. The time and expense involved may be prohibitive.
ii. Second, the physical presence of an adversary is a concern because these devices can be exchanged or tampered with or used to introduce false information into the system to cause a direct failure.

Unencrypted Data: As often occurs in M2M devices, data encryption is omitted from embedded systems. With access to any particular end point or data point, it is not difficult to put a sniffer on that network, intercept network traffic over a variety of different protocols, and figure out how to exploit that information.

Industrial Control Systems: An Example of Expanded Attack Surfaces in M2M Environments

Industrial control systems (ICS) and SCADA systems used in everything from vehicle manufacturing to energy plants are at particular risk for security threats. When these systems were developed and deployed, the critical embedded systems within them were created with a focus on uptime and cost control; security was not a priority. The lifespan of this equipment is often 20 years or longer, so as they are upgraded and come "online" they become susceptible to all of the risks that come with connectivity. The Human Machine Interface (HMI) represents a point of potential compromise. Because these systems are often older and upgraded over time, the risk is compounded by old operating systems, un-patched software and legacy applications.

5.6 Challenges - Security

The IoT is where the Internet meets the physical world. A major disruption of the traditional model for the new brings its own set of challenges. The following lists some security challenges and considerations in designing and building IoT devices or systems:

i. Typically small, inexpensive devices with little or no physical security.
ii. Though inexpensive, every device still has to compute something and also have some security feature. Also, it should not add to latency in processing.
iii. Computing platforms, constrained in memory and compute resources, may not support complex and evolving security algorithms due to the following factors:
    - Limited security compute capabilities.
    - Encryption algorithms need higher processing power
    - Low CPU cycles vs. effective encryption
iv. Designed to operate autonomously in the field with no backup connectivity, if primary connection is lost.
v. Mostly installed prior to network availability which increases the overall onboarding time.
vi. Requires secure remote management, up-dating during and after onboarding.
vii. Scalability and management of billions of entities in the IoT ecosystem.
viii. Identification of endpoints in a scalable manner, Sometimes the location may be more important than the individual identifier (ID).
ix. Management of Multi-Party Networks.
x. Crypto Resilience
    - Embedded devices may outlive algorithm lifetime.
    - Crypto algorithms have a limited lifetime before they are broken
xi. Physical Protection
    - Mobile devices can be stolen
    - Fixed devices can be moved
xii. Tamper Detection techniques and design

- Always On: High Poll rate, more energy, quick detection.
- Periodic Poll: Less energy, slower detection
- On-event Push: Minimal energy, no detection

The IoT entities will generally not be a single use, single ownership solution. Consequently, Identification and authorization of M2M devices in a dynamic and autonomous world will pose serious research challenges. Authentication mechanisms should work side-by-side with distributed trust management and verification mechanisms. Any two M2M devices should be able to build and verify a trust relationship with each other, and this problem is certainly more challenging in environments without a security infrastructure in place. Trust will be an important requirement for designing new identification and authentication systems for M2M.

As authentication is related with identification, M2M systems will probably need to incorporate some type of secure identifier, tying information identifying the device or application with secret cryptographic material. Current proposals point to the usage of ITU-T specified X.509-based certified secure identifiers, for example using IEEE 802.1AR, or on the other end of self-generated uncertified secure identifiers, also called cryptographically generated identifiers, for example, the use of private keys in GSM Network authentication.

As M2M systems require that privacy is balanced against disclosure of information, new authentication mechanisms relying on appropriate secure identifiers and incorporating privacy-preserving mechanisms are required. This aspect may also be incorporated in new trust computation mechanisms, as the evaluation of the risk in accepting communication with a partially unknown device may also consider the level of privacy accepted for an M2M application.

As distributed and autonomous trust mechanisms will be required for M2M environments, trust must be established on an M2M device from the start. Local state control via secure boot (local trust validation) may be enforced for M2M devices, similar to the mechanisms previously analyzed in the context of the ETSI M2M architecture. This secure boot may allow the establishment of a trusted environment providing a hardware security anchor and a root of trust, from which different models for trust computation may be adopted. In this context, the Trusted Computing Group (TCG) has proposed autonomous and remote validation models.

Autonomous validation (for example: using smart cards storing authentication secrets) presents the problem of requiring costly in- field replacements of compromised devices. Remote validation presents problems related to scalability and complexity, regarding limitations of M2M devices.

A promising avenue for research in this field may be that of semiautonomous validation. Semiautonomous validation combines local validation with remote validation, meaning that a device is able to validate trust for another device and communicate with a trusted third-party in situations of absolute necessity (in many environments such third party may not be available at all). Distributed semiautonomous trust verification mechanisms are therefore necessary for M2M environments. The previously described M2M architecture from ETSI also incorporates the usage of secured and trusted environment domains, controlled by the M2M service, as a cornerstone for the (secure) usage of security credentials on M2M devices and gateways.

5.7 Challenges - Authentication and Authorization

Authentication

At the heart of IOT secure framework is the authentication layer, used to provide and verify the identify information of an IoT entity. When connected IoT/M2M devices (e.g., embedded sensors and actuators or endpoints) need access to the IoT infrastructure, the trust relationship is initiated based on the identity of the device. The way to store and present identity information may be substantially different for the IoT devices. Note that in typical enterprise networks, the endpoints may be identified by a human credential (e.g., username and password, token or biometrics).

The IoT/M2M endpoints must be fingerprinted by means that do not require human interaction. Such identifiers include radiofrequency identification (RFID), shared secret key, X.509 certificates, the MAC address of the endpoint, or some type of immutable hardware-based root of trust. Establishing identity through X.509 certificates provides a strong authentication system. However, in the IoT domain, many devices may not have enough memory to store a certificate or may not even have the required CPU power to execute the cryptographic operations of validating the X.509 certificates (or any type of public key operation).

Existing identity footprints such as 802.1AR and authentication protocols as defined by IEEE 802.1X can be leveraged for those devices that can manage both the CPU load and memory to store strong credentials. However, the challenges of the new form factors, as well as new modalities, create the opportunity for further research in defining smaller footprint credential types and less compute intensive cryptographic constructs and authentication protocols.

Authorization

The second layer of this framework is authorization that controls a device's access throughout the network fabric. This layer builds upon the core authentication layer by leveraging the identity information of an entity. With authentication and authorization components, a trust relationship is established between IoT devices to exchange appropriate information. For example, a car may establish a trust alliance with another car from the same vendor.

That trust relationship, however, may only allow cars to exchange their safety capabilities. When a trusted alliance is established between the same car and its dealer's network, the car may be allowed to share additional information such as its odometer reading, last maintenance record, etc. Fortunately, current policy mechanisms to both manage and control access to consumer and enterprise networks map extremely well to the IoT/M2M needs. The big challenge will be to build an architecture that can scale to handle billions of IoT/M2M devices with varying trust relationships in the fabric.

5.8 Challenges - Heterogeneity and Resource Constraints

Given the limitations on the computational capabilities of many sensing and actuating platforms, security technologies must be developed to cope with and supported by architectures with the characteristics similar to the ETSI M2M architecture. For example, applications using passive Radio-Frequency Identification (RFID) tags are unable to support security mechanisms requiring the exchange of many messages and communication with servers on a network domain.

Lightweight solutions for symmetric and asymmetric cryptography which have been proposed in recent years provide a useful guidance in this context. The heterogeneity of sensing/actuating M2M devices may also be addressed by security approaches at higher layers of the protocol stack or at the middleware, in line with the approach previously discussed regarding Identification, authentication, authorization and trust.

5.9 Challenges - Privacy and its Preservation

Privacy is one of key importance nowadays. People are concerned about their personal data that is on the internet. The right to privacy in India has developed through a series of decisions over the past 60 years. In an unanimous judgment by the Supreme Court of India (SCI) in Justice K.S. Puttaswamy (Retd) vs Union of India, in August 2017, has ruled that the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution. Enterprises try to protect their information, communication and application infrastructure, causing them to have private mail servers, data storages etc. Privacy can be divided into a few categories that have unique technical aspects:

(i) Communication privacy

(ii) Position privacy (Location privacy)
(iii) Path privacy
(iv) Identity privacy (Personal privacy)
(v) Personal data (use crypto for data protection)

Sticky policies are a way to cryptographically associate policies to encrypted (personal) data. These policies function as a gate keeper to the data. The data is only accessible when the stated policy is honoured. System keeps track of personal data relating to the user, as well as applied policies and service customizations.

An imperative aspect of IoT technology is their ability to connect the physical world to the digital world. M2M applications may also require the control autonomous M2M device-to-device identification and authorization.

For some M2M applications (in the context of the IoT) the user will require to be able to control the amount of personal information exposed to third parties, for instance in maintaining privacy while exposing personal records in healthcare applications. On the other end, other M2M applications may require that some of that information is available in case of necessity, for instance with M2M vehicular applications in case of traffic accidents.

Privacy Preservation

Preservation of privacy has been a concern since the dawn of the Internet. IoT will exacerbate the problem because many applications generate traceable signatures of the location and behaviour of the individuals. Privacy issues are particularly relevant in healthcare, and there are many interesting healthcare applications that fall within the realm of IoT. In this environment, it is essential to verify device ownership and the owner's identity while decoupling the device from the owner. Shadowing is a mechanism that has been proposed to achieve this. Identity management in the IoT may offer new opportunities to increase security by combining diverse authentication methods for humans and machines. Privacy and compliance are intertwined and are under the purview of country regulation

Security and privacy

The various challenges posed to the addressing of security in M2M may benefit from a paradigm shift in how the various security requirements are guaranteed. For example, scenarios without a security infrastructure in place may consider classic security solutions side-by-side with new decentralized and distributed approaches. As in other scenarios M2M systems may be unable to derive definitive conclusions about the identity or intents of other devices, security mechanisms may need to consider compromises between the enforcement of definitive security controls and the acceptance of controlled risks

Other aspects are trust and privacy, which may motivate the design of new security mechanisms and approaches. Distributed and autonomous trust management and verification mechanisms will be required to support autonomous M2M device-to-device identification and authorization.

M2M applications may also require the control of privacy and liability, as previously discussed. For some M2M applications (in the context of the IoT) the user will require to be able to control the amount of personal information exposed to third parties, for instance in maintaining privacy while exposing personal records in healthcare applications. On the other end, other M2M applications may require that some of that information is available in case of necessity, for instance with M2M vehicular applications in case of traffic accidents. Challenges also exist in the usage of M2M architectures such as the one from ETSI, side-by-side with emerging communication and security solutions.

5.10 Challenges – Identity, Anonymity and Liability

M2M Connectivity requires that the user and the use case be identified. This leads to the requirement of requesting and storing user and machine credentials. With that said, comes the challenge of maintaining anonymity of this ‘identity’ related information.

As previously discussed, anonymity and liability are two interrelated security requirements for M2M applications. Such requirements are not only related with security, but they are also vital for the social acceptance of many applications envisioned for M2M.

Anonymity is necessary as applications may only be accepted if the user is guaranteed to have a certain degree of protection of its personal (or other) information. Liability is a deeply related requirement, as other applications may require access to private information in case of necessity, for example for legal purposes. As anonymity will be required in M2M, research can target the applicability of light weighted formal anonymity models such as k-anonymity to M2M environments.

Possible alternative approaches are the development of mechanisms for data transformation and randomization. Intrusion detection will also be relevant for autonomous M2M environments. Autonomous and cooperative methods allowing the early detection of node compromises may be the path to follow in this domain.

5.11 Mitigation of IoT/M2M Security Threats and Risks

Mitigating the Risks

The four guidelines that embedded software teams should follow to help protect critical M2M systems against failure and malicious attack are:

1) Address security early and take defensive measures against security threats using threat modelling.
2) Reduce Security risk as enumerated below:
3) Build security in at the development stage by finding and fixing code vulnerabilities with static analysis and code review.
4) Protect systems Through Secure Analytics: Visibility and control.

5.12 Address Security Early: Threat Modelling

Securing an M2M system starts with understanding the potential threats. Threat modelling involves thinking about the system or asset that needs protection and identifying how it can be compromised, either by remote attack or by a malicious insider. Threat modelling therefore begins in the software architecture stage and continues through the design phase.

Once the risks are understood, proactive measures to create a risk mitigation strategy can be made. When conducting this activity, it is important to remember that threats are not vulnerabilities. Vulnerabilities can be fixed; threats exist in perpetuity and are the attacker's goal. Considering potential use and abuse cases will help you to determine threats and attack vectors on which to base a threat model. These include:

(i) Data: Consider not only the data on the device, but also the data in connected systems that the device is able to access.
(ii) Input Sources: Study the various input sources that could be used to attack a device. This may include wired and wireless networking, Bluetooth, GPS signals, cellular voice/data, remote controls, etc.
(iii) Environment: Look at how to protect data? Should there be the physical presence of an adversary? Or should the device be used outside of normal expectations?

While the industry will evolve and embrace interoperability and platform standards, it also needs to integrate core trust principles. These cannot be bolted on mid-flight, and instead must be designed in from the onset. Creating a culture of security, privacy and sustainability with transparency will yield long-term benefits to society. Through working groups and strategic relationships with subject matter experts in interactive marketing and advertising, technology, privacy and public policy, OTA provides strategic insights helping members prosper and innovate as thought leaders while avoiding potholes and roadblocks.

When designing the system, threat should be analysed from the perspective or point of view of an attacker. Threat modelling, also called Architectural Risk Analysis, is a security control to identify and reduce risk. An example of Threat Modelling is the STRIDE Threat Model (Figure 13) as per Wikipedia, STRIDE is a threat classification model developed by Microsoft), which helps place threats into categories such as Repudiation, Information disclosure, Tampering with data, Denial of service, Spoofing identity etc, and it includes a full breakdown of processes, data storage, data flows and trust boundaries.

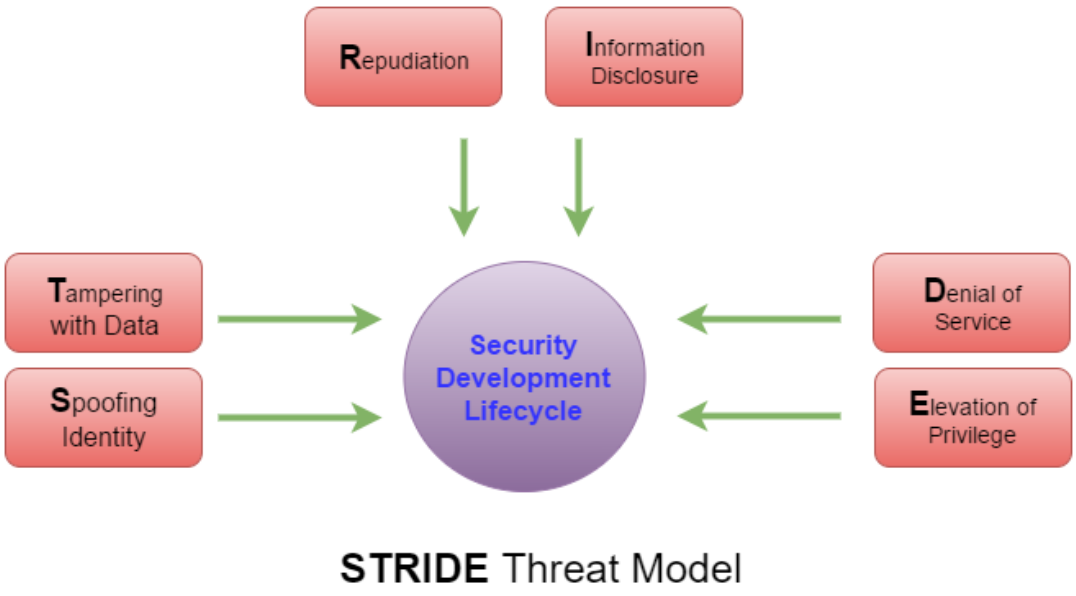


Figure 13: STRIDE Threat Model

5.13 Reducing Risk

There are a number of opportunities to minimize risks to M2M embedded systems:

Attack Surface

The entire collection of entry points into a system or device defines its attack surface. The larger the attack surface, the greater the potential security risk. Analyzing the attack surface allows engineers to gauge risk and uncover potential avenues of attack.

Reducing the attack surface naturally limits the number of attack vectors or entry points into an embedded system. This does not negate the need to investigate all routes into a device (including user interfaces, network access, web services, etc.) and to analyze the attack surface of all third-party components in use as well.

Secure Design

The secure design of M2M embedded systems relies heavily on a number of crucial elements being applied at the development stage:

(i) Enforce Boundaries: Isolate code to enforce strict boundaries between the operating system and the process.

(ii) Protect Data: Encrypt data in transit. Protect data at rest using the underlying file system encryption features and employ separate keys.

(iii) Enforce Least Privilege: Ensure that every program and every user of the system operates using the least set of privileges necessary to complete his/her/its job.

(iv) Perform Integrity Checks: Always perform integrity checks to validate authenticity—embedded devices usually rely on firmware updates.

(v) Non-Repudiation: Use a data hash, such as SHA2, to establish the authenticity of the data.

(vi) Use Modular Cryptography: When employing cryptography, assume that algorithms will be replaced over time. Keep code modular and avoid custom algorithms.

(vii) Protect Against Denial of Service: Use solid system management and software design to avoid resource exhaustion and vulnerability to Denial of Service attacks.

(viii) Authenticate: Make authentication strong and manage it centrally to ensure inputs are from trusted sources.

5.14 Build Security In

Security vulnerabilities in embedded software have two sources:

(i) Design flaws and fundamental approach problems

(ii) Coding issues/bugs and bad programming practices

Because the applications and devices at the end of every connection are presumed trustworthy in an M2M environment, the responsibility rests with the development team to ensure the security of embedded software. Build Security In by

A. Code Signing

Code signing is the process of digitally signing an object, such as executable code or configuration data. Signing can be used to confirm the source of firmware and guarantee its integrity to ensure it has not been altered en-route to the device, and is crucial for deploying firmware in distributed environments. It is important to note that code signing relies on traditional public-key cryptography and is only as secure as the private keys. Signing guarantees unaltered code, but does not guarantee secure code.

B. Find and Fix Security Vulnerabilities: Static Analysis

From the architectural design process through to the coding process, tooling is a proven way to help reduce security weaknesses.

A static analysis tool enables embedded software development teams to find hundreds and thousands of problems with code throughout the stack, including traditional weaknesses, reliability concerns, long-term cost of ownership, 'bad smells', code style or coding standards violations, and even layout issues. By using static analysis, development teams can focus their efforts on the high-value or high-return vulnerabilities—the ones they know are common in the embedded space—such as uninitialized data, use of dangling pointers, injection vectors, and use of "known" insecure APIs and libraries.

Static analysis can also help embedded software developers deal with well-known but hard-to-understand security vulnerabilities.

Take the buffer overflow as an example. A buffer is a fundamental part of the C/C++ language, but when a buffer of insufficient size is used to copy into memory, this practice can make code vulnerable. Buffer overflows cover so many different forms of exploits that it's almost impossible to quantify. This is demonstrated by how frequently buffer overflows are named as the culprit in security breaches. The issue isn't that developers don't understand what a buffer overflow is; but that, as the size and complexity of a code base grows and as development teams work on solving increasing complex problems, these types of vulnerabilities become more sophisticated and increasingly harder to find.

With static analysis tools, these issues are identified and explained in a way that helps developers fix them early in the development process. The closer the analysis is run to the developer, the sooner any issues can be fixed. Ideally, static analysis is running at the same time that developers are coding to ensure that security vulnerabilities are found and fixed before code check-in.

C. Conduct Effective Code Reviews

In addition to static analysis, peer code review is an important and extremely valuable tool in helping ensure that security vulnerabilities don't make it into the field. By identifying bugs and design flaws, and ensuring coding standards and best practices are being followed, code reviews create consistency and a culture of quality. By sharing knowledge with others and learning from identified mistakes, developers also become better programmers. The practise of code review has been embraced by development organizations. Around 87% of respondents in response to a commissioned study conducted by Forrester Consulting, said that code review is mandatory in their organization. Unfortunately, the traditional approach to code reviews is not as effective as it could be:

(i) Scheduling troubles: It is difficult to get all the right people in a room at the same time, and near impossible when those teams are geographically distributed.

(ii) Unprepared participants: Sometimes developers are not prepared for a code review meeting, either because they don't understand what code was changed or why, or did not have the time to review the code in question in advance of the meeting.

(iii) Time-consuming: In a group setting, it can take hours to review only a couple hundred lines of code.

(iv) Missing issues: Thinking "on the spot" without proper preparation leads to overlooked issues, with the industry standard showing code reviews as being only 55-60% effective. While it's hard to get right, implementing a solid code review process can have a significant impact on code security.

Tools that allow individual developers to contribute to code reviews via their desktops, when it's most convenient for them is an ideal approach for reaping the rewards of this practise. A study conducted by the Royal Military College of Canada found that at-desk code reviews are 50% more effective than traditional sit-down meeting code reviews

5.15 Secure Analytics: Visibility and Control

This secure analytics layer defines the services by which all elements (endpoints and network infrastructure, inclusive of data centers) may participate to provide telemetry for the purpose of gaining visibility and eventually controlling the IoT/M2M ecosystem. With the maturity of big data systems, we can deploy a massive parallel database (MPD) platform that can process large volumes of data in near real time. When we combine this technology with analytics, we can do some real statistical analysis on the security data to pick out anomalies.

Further, it includes all elements that aggregate and correlate the information, including telemetry, to provide reconnaissance and threat detection.

Threat mitigation could vary from automatically shutting down the attacker from accessing further resources to running specialized scripts to initiate proper remediation. The data, generated by the IoT devices, is only valuable if the right analytics algorithms or other security intelligence processes are defined to identify the threat. We can get better analytical outcome by collecting data from multiple sources and applying security profiles and statistical models that are built upon various layers of security algorithms.

5.16 Securing IOT/M2M-Security features and counter measures

With data sharing across the IoT, security is a necessary part of every activity of every cooperative initiative, regardless of use case. There are already too many possible points of entry for security to be airtight, and with the IoT, these will be multiplied exponentially. Each company may require unique security solutions to address its own set of risks. The most immediate imperative is to verify software and ensure that security controls are able to address the latest risks and a plan is in place for responding to new risks in a timely fashion. Put in place encryption and/or strong session management security controls and Implement secure coding practices that enforce rigorous input data validation in system and services, database applications, and web services.

Implementing security features and countermeasures to threats requires mechanisms that provide security related operations with an appropriate level of confidence. The generic mechanisms are described within this include:

(i) secure storage of sensitive data
(ii) sensitive functions executing operations on sensitive data
(iii) secure connection allowing the secure transmission of sensitive data

Sensitive functions are typically performed in termination points within the M2M System. Examples of sensitive functions include:

(i) cryptographic algorithms (session) key derivation functions
(ii) hash functions

Thus the mechanism exploits the use of two fundamental cryptographic primitives: hash functions and public key systems. In general, cryptographic functions operate on inputs such as messages and keys, and produce outputs such as cipher texts and signatures. Public key encryption relies on a pair of related keys, one secret and one public, associated with each individual participating in a communication. While slower than secret key cryptography, public key systems are preferable when dealing with networks of devices that need to be reconfigured fairly often.

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. A detailed risk assessment/evaluation of the level of impact of the threat depends on the assets and their value. The security affected in the various domains includes:

(i) Application domain security;
(ii) Intra Common Services domain security;
(iii) Inter Common Services domain security;
(iv) Underlying Network security, if keys are shared with underlying network.

Securing an M2M system starts with understanding the potential threats. Threat modelling involves thinking about the system or asset that needs protection and identifying how it can be compromised, either by remote attack or by a malicious insider. When conducting this activity, it is important to remember that threats are not vulnerabilities. Vulnerabilities can be fixed; threats exist in perpetuity and are the attacker's goal. The aspect concerning the securing of M2M/IOT subsystems are discussed in greater detail in the subsequent chapters which deal with Network layer security and Application domain security.

6. Summary of Inputs from Work Groups

The Security Work Group distributed the said threats and challenges for review amongst the sub-working groups. The section below summarises the output from the deliberations within the sub-work groups. The reader may please note that the recommendations in this section, are interim results of the assessment within the sub-groups. The final recommendations of the Working Group are in the section 7 of this report.

6.1 Sub Group-1: End Point Devices Security

Summary of Recommendations of SWG 1: End Point Devices 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.

6.1.1 Levels of Assurance

This report proposes the following Assurance Levels for End Point Devices:

Level 0 (No security)

This state of security defines no standard security; this is for non-standard END_POINT devices having no identical identification and even not assigned its identifier using standard norms. This could be under Low energy product (Bluetooth, ZigBee) and used for limited scopes.

Best use case for device that could be under a close circuit infrastructure behaving as child and only responsible to its parent node.

Level 1 (Device recognition)

END_POINT devices must have their unique identity to recognize them in network, whether it is low energy or in cellular. It does not have inbuilt security features but device can be identified and helps the server to utilize devices with full functionality and even devices could be recognized for their specific function and specific location.

Level 2 (Device verification)

In this level of security identification and verification is included. Verification process is based on traditional OTP. This verification stops the misuse of END_POINT device and could be personalized and activated based on its verification.

Level 3 (Secured device verification using username password)

Traditional authentication systems are based on user name and password. It needs secured communication between the device and serving system as well device identification using IP address and device ID.

Level 4 (Device Identification and authentication)

Device identification and its authentication with PKI infrastructure will be added in this level of security, best use of these END_POINT devices would be in cellular. Its functionality is integrated with eUICC. The authentication is based on cellular identification and authentication system following 3GPP standards.

Level 5 (Biometric authentication and Personalization)

In this state of security biometric data could be used authenticate personal END_POINT device to restrict unauthorized usage of devices and its produced data. The best use case for this kind of device in eKYC.

The diagram (Figure 14) below represents the 5 levels of security defined in the document:

Biometric data could be used for device authentication as well as user authentication.

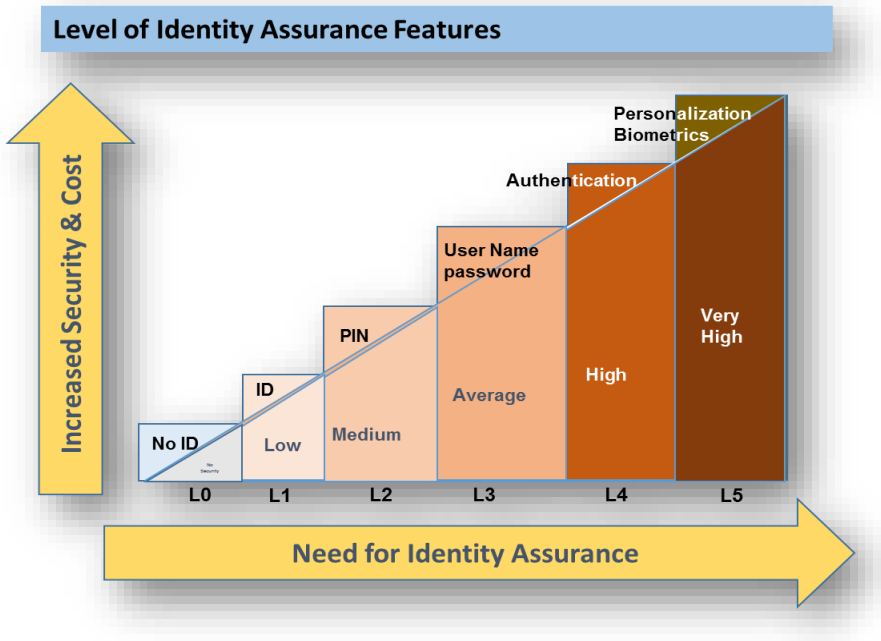


Figure 14: End Point Assurance Levels

Level 0: No authentication and Identification

Level 1: Identification and Authentication based on defined ID on End Point Device

Level 2: PIN based Authentication and Identification

Level 3: User name and password authentication method

Level 4: By Key exchange and mutual authentication method

Level 5: Biometric authentication

The table below (Figure 15) recommends certain options for user authentication based on the classification of the Assurance Levels for End Point Devices.

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

Figure 15: Assurance Levels for End Point Devices.

6.2 Subroup-2: Network Communication Security

Summary of Recommendations of SWG 2: Network Communication Security

- The network supporting M2M services, even if it is being provisioned using unlicensed spectrum should be subjected to Licensing obligations.
- Suitable guidelines be stipulated, similar to the GSMA guidelines for remote provisioning and management of machine to machine (M2M) connections Over The Air (OTA) for provisioning of an operators' subscription in eUICC / embedded SIMs, for prevention of SIM cloning / destruction.
- 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.
- Since, the usage of M2M services closely shadow their owners' characteristic, it is suggested that the end to end M2M services setup, for provisioning M2M services in India, should mandatorily be hosted in India.
- The SIMs of foreign TSPs should be mandated to be converted to domestic TSP SIMs within a period of 1 year from the date of activation of the device in India.
- India needs to negotiate maximum number of MLAT agreements to ensure optimal utilization of the M2M eco-system.
- MCC and MNC should not be directly allocated to the MSPs.
- M2M SIMs, being industrial grade, are costlier than the normal SIMs hence, these should be permitted to be procured by the MSPs.
- For ensuring adequate redundancy and making the M2M services connectivity robust and TSP agnostic, MSPs should be permitted to interface their data gateway with multiple TSPs.

6.3 Sub Group-3: Application Level Security

Summary of Recommendations of SWG 3: 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.

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.

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.

To ensure the Application Layer Security for M2M domain, it is proposed to have the following Registration procedures

- Registration and Identification of the M2M Service Provider and M2M Application Service Provider by a Registration Authority

- Registration and Identification of the Common Platform Layer and the Application Layer Instances by the National Trust Centre

- Registration and Identification of the End Point Devices by the National Trust Centre

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). 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.

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. It also enables to keep control over applications issued by untrusted sources. In this regard, it is important to ensure that the standards and policies mandate how secured credentials such as Aadhaar or Digital Certificates may be used for binding Users to the M2M applications they have access to through a KYC/e-KYC verification.

The M2M Service Providers should be required to publish periodic customer and End Point data to the M2M Registration Authority / National Trust Centre, as also to expose secure web access with authorised credential for Law Enforcement Agencies to verify the Users / End Points / Application Usage data when authorised by the law.

The M2M Application Enrolment procedure should enable the M2M SP and/or M2M application service provider to control which applications are allowed to use the M2M services. The M2M applications User must obtain and register its credentials, which must be verified each time for controlling authorization/ access to M2M Applications. Each M2M application should be provisioned with a security credential (M2M Application key) which can be used to grant specific authorization to access an approved list of M2M services.

To practically achieve the above objectives, whilst ensuring that M2M applications remain inter-operable, scalable, sustainable and secure, architecture with a separated Common Platform layer and Application Layer becomes necessary. Such architecture is described in the figure 16 below:

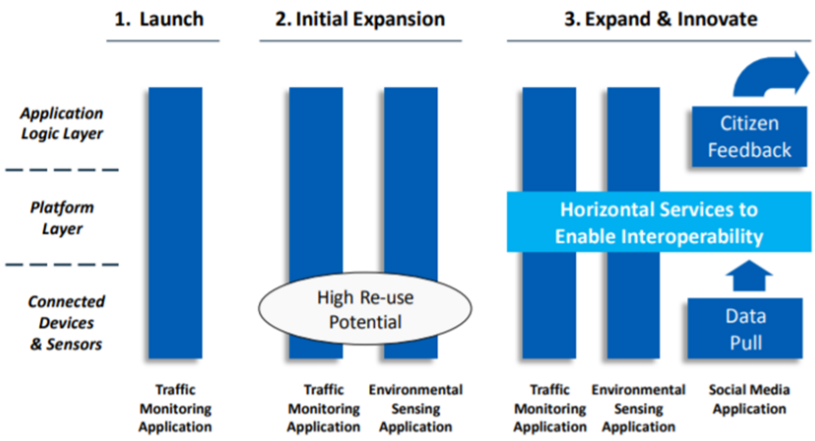


Figure 16: Phased Evolution Approach, The 4th Industrial Revolution, ETSI White Paper No. 26

In the architecture proposed above, End Point Application Instances (EPAIs) are authorized by a registration to the Platform Layer Instance (PLI). As a result, the PLI becomes responsible for the Identification and Authorisation of the EP.

Now, since it is described how the three actors namely, the End Points, the Platform Layer Instances and the Application Layer Instances are registered and recognised, the following mandates should be provided for implementation of M2M Security

- The Platform Layer must implement an authentication function for identifying and authorising EPs with the associated M2M service subscription

- The authentication function must validate the credentials provided to the EPs during the M2M application enrolment procedures for granting access to M2M services

- Upon mutual authentication of the EPs with the M2M Platform Layer, the corresponding End Points receive authorization to access the M2M services defined in the M2M Service Subscription

- It must be mandatory to establish a Secure Association by generating a security credential (M2M Connection key), which must be shared between communicating End Points / Platform Layer when an End Point / Application on one node initiates communication with an End Point / Application on another node

- This procedure is performed after successful identification and mutual authentication of the corresponding M2M Nodes which is necessary to provide access to the desired security services to the communicating entities, such as confidentiality and/or integrity of information exchange (these security

services may be provided through establishment of a secure channel between the communicating entities or through object based security where only relevant information is encrypted prior to being shared).

- The lifetime of a security association must be shorter than the lifetime of the credential used for authentication from which it is derived. It may be valid for the duration of a communication session, or be determined according to the validity period of the protected data.

- In case of a security association between two Application Instances, the lifetime of the security association can result from a contractual agreement between the subscribers of the communicating Application Instances.

In view of the aforementioned background, the following requirements must be fulfilled for M2M Access Control, Authorisation and Security:

- Horizontal Security requirement for the Applications hosted in the Applications Logic Layer

    - Use of Security Associations, mutual Authentication and Confidentiality
    - Session Management and detection of Broken Authentication
    - Resistance to Man-in-the-Middle Attacks
    - Limited Life Session Keys bound to Service Layer
    - Replay protection
    - Secure Coding Rules and strong application architecture with good separation and security between components
    - Limited number of Batch Actions
    - Limited functionality for APIs
    - Whitelisting capability for limiting access to/by URLs / IPs, including APN control for 3GPP enabled use cases
    - Remote locking of the Connectivity Element Identity with Device / Asset Identity (e.g. locking of IMSI with Device IMEI for 3GPP enabled use cases)
    - Remote and Secure updates of security parameters in EP Firmware/EPAIs such as Keys, IPs, APNs etc

- Minimum requirements for the Authentication Functions within Applications Logic Layer

    - Role Based Access Control
    - Token based Authorisation e.g. OAUTH
    - Context based Access Control under control of Owner e.g.
    - Granting Access to Digital lock in case of an emergency
    - Granting Access to Home Gateway for Service

- Minimum requirements for the interaction between Application Entities and End Points

    - A minimum use of Private or Public Keys for Gateways
    - 3DES / AES / AKA algorithms for hashing, encryption and signing
    - Support for Key Generation, Transfer, Storage, Revocation
    - Identification and Encryption of Sensitive and PII data, Secure storage of Sensitive Application Data
    - Mechanisms for generating Application Layer alerts when QoS and Reliability conditions are not met
    - Health Packets and Heartbeat mechanisms between End Points and Applications for mission critical applications
    - FMEA and Analytics in order to anticipate and analyse breakdowns
    - Ensuring compliance to DoT / MIETY Guidelines for storage of Data in India
    - Identification of the IPs / Location of Application Servers, Platforms and Network Elements
    - Minimum Data Retention and Archival as per Standards and Guidelines relevant to the Use Case
    - Lawful Interception capabilities
    - Protection of Storage by privileges
    - Management of Sensitive functions executing operations on sensitive data including prevention of Cross Scripting / Application ID Spoofing
    - Device Management Function to ensure that configuration of End Points is not amended without the explicit permission of the M2M SP / Device Owner e.g.
    - Configuration of Home Security Devices

- Frequency of Data Submission, IP for Data Submission in case of VTS devices
- Configuration of IPs to which Device Sends Data
- Configuration of IPs within APNs from which data can be accepted
- Functionality for identification and reporting for unauthorized or corrupted Applications or Software in M2M Devices/Gateways
- Blocking of Services until E-KYC registration is completed

As per GSMA's IoT Security guidelines, Application Security for mission critical and sensitive applications requires compliances to address the challenges of Availability, Identity, Privacy and Security. The following two approaches are recommended for addressing the said challenges:

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

  - Another major development for IoT / M2M use cases is the GSMA eSIM
  - The eSIM can be used to mitigate all the major challenges identified by the GSMA IoT Security Guidelines
  - Availability is ensured with multi-profile, remote provisionable eUICC
  - The solderable form factor of the eSIM can provide a unique tamper proof identify for the EP
  - The secure element and key stored within the eSIM can be used to ensure privacy by signing the messages and transactions
  - The eSIM Secure Element can be used for end to end encryption / decryption within EPs whose low end controllers cannot handle the high end security features
  - The embedded form factor of the multi-profile eSIM / Remote Provisionable eUICC should be recommended for all use cases that are sensitive to privacy and require end to end security and high quality of service

- Generic Bootstrapping for Access Control

  - A convenient and inexpensive method to introduce security in M2M Use cases, in scenarios where the M2M Service Provider and the Network Service Provider (operator of the underlying network) have an agreement, is to use the underlying network credentials as the basis for security between a M2M Application Service, M2M Platform Layer and the End Points.
  - In this Architecture, a generic Bootstrapping Server Function (BSF) and the EP shall mutually authenticate using the AKA protocol and agree on session keys that are afterwards applied between EP and a Network Application Function (NAF). The BSF shall restrict the applicability of the key material to a specific NAF by using the key derivation procedure as specified in the relevant 3GPP Standards. The key derivation procedure may be used with multiple NAFs during the lifetime of the key material. The lifetime of the key material is set according to the local policy of the BSF
  - The Figure 17 below shows a generic Bootstrap Architecture as per ETSI

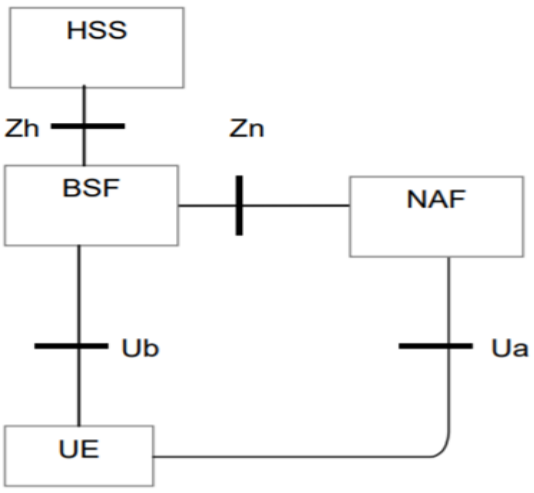


Figure 17: Generic Bootstrapping for Access Control

6.4 Sub Group-4: Trusted Environment

Summary of Recommendations of SWG 4: Trusted Environment

Trust in ICT Environments

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.

Trust can be classified into two broad categories: “user” and “system”. The notion of “user trust” is derived from psychology and sociology, with a standard definition as “a subjective expectation an entity has about another’s future behaviour.” “System trust” is “the expectation that a device or system will faithfully behave in a particular manner to fulfil its intended purpose.

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. Various components of security, which should be taken care of for building trusted environment are shown in the diagram (Figure 18) below

Figure 18: Trusted Environment

Physical Domain trust

A physical domain contains a huge number of objects (i.e., H/W or device) including sensors, actuators, mobile terminals, which generate data by using sensing technologies to sense physical objects and their behaviours within their environments (e.g., temperature, pressure, etc.). Collecting secure and reliable data from physical objects is the first step to provide trustworthy ICT services and applications because the propagation and process of false data will cause service degradation and waste system resources.

Cyber trust

A cyber domain includes virtual objects such as software agents, services and applications working over computing, storage and networking components. These virtual objects are seamlessly interconnected and cooperated for data coding, transmission, fusion, mining and analysing to provide information and knowledge to humans independent of location in fixed/mobile environments.

Cross-domain service trust

Trust management is service and domain specific, and it may be desirable to combine features from different trust management systems for developing cross-service trust management which is able to cover social-cyber-physical trust relationships between different service domains.

• Trust IdM: The identity management (IdM) can be used to manage digital identification/authentication of social-cyber-physical objects. Trust IdM assures the identity of trustworthy objects and support trust-based services.

• Trust Data Repository: The trust data including operations of objects and the history of interactions between objects can be maintained in the trust data repository. For trust evaluation, the necessary data will be loaded from this repository to the computation module.

• Trust Computation: This module is used for data processing for trust evaluation. Trust computation happens when the state of an object is changed or an interaction occurs between objects. To process a large amount of data related to trust evaluation, it can adopt data analytics and cloud computing technologies for calculation of the trust level of objects according to the change of the trust state of objects based on direct observation.

Trust Framework

The IoT Trust Framework includes principles, segmented into four key categories:

(i) Security - Applicable to any device and their applications and backend cloud / backhaul / access / storage/ processing / gateways communication services. These include embracing a rigorous planning, development, implementing, operating security process, adhering to security principles for data stored and transmitted by the device, supply chain management, penetration testing and vulnerability reporting programs.

(ii) User access & credentials - Requiring encryption of all passwords and usernames, implementing devices with unique passwords, implementing generally accepted password reset processes and integrating mechanisms to help prevent brute force login attempts in devices, aggregation platforms, communication nodes , processing platforms etc.

(iii) Privacy, disclosures & transparency - Requirements consistent with generally accepted privacy principles including prominent disclosures on packaging, point of sale and/or posted online. Provide the capability to reset devices to factory settings and be in compliance with applicable regulatory requirements.

(iv) Notifications & related best practices - Key to maintaining device security is having mechanisms and processes to promptly notify a user of threats and action(s) required.

Role of service provider in M2M system and trusted system creation

• While, M2M endpoints and M2M gateways might be dedicated to specific M2M services, M2M systems as a whole will frequently share resources with a variety of other un-related systems and applications

• Application domain security, intra common services domain security, inter common services domain security, underlying network security as indicated earlier assume great importance to keep track of the entire ecosystem .

• Also, as mentioned, though M2M nodes in the field domain are assumed to communicate without human involvement, individuals or organizations remain responsible for setting the access control policies used to authorize their M2M nodes to access M2M services. Framework of Trust Management of IoT is shown in the diagram (Figure 19) :

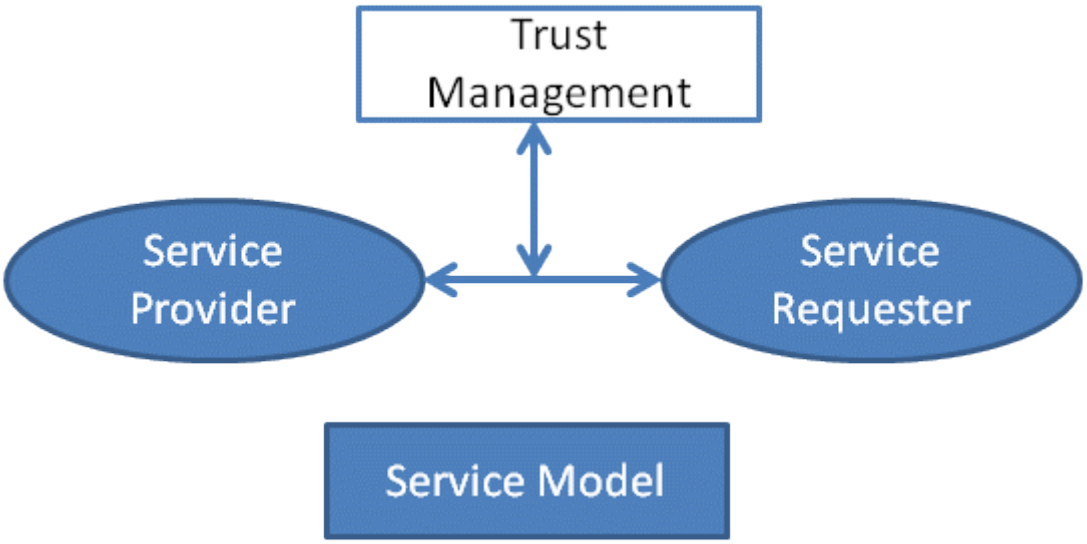


Figure 19: Framework of Trust Management

In particular, individuals or organizations acquiring M2M nodes can subscribe to a contract with an M2M Service provider (M2M Service Subscription) under which they enrol their M2M nodes. This in turn may require an M2M Service provisioning step (including Security provisioning) that takes place on the target M2M nodes themselves, for which interoperable procedures are specified by standards like oneM2M. Following M2M service provisioning, the nodes 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.

Similarly, it can be possible for an M2M service provider to mandate that application accessing M2M services be provisioned with security credentials used to authorize specific operations to instantiated applications. As in some scenarios M2M systems may be unable to derive definitive conclusions about the identity or intents of other devices, security mechanisms may need to consider compromises between the enforcement of definitive security controls and the acceptance of controlled risks. That is closer to trust concept! The diagram (Figure 20) below shows the model for security for Multiple security vendors platform, wherein each individual organization should verify each other organization's trustworthiness.

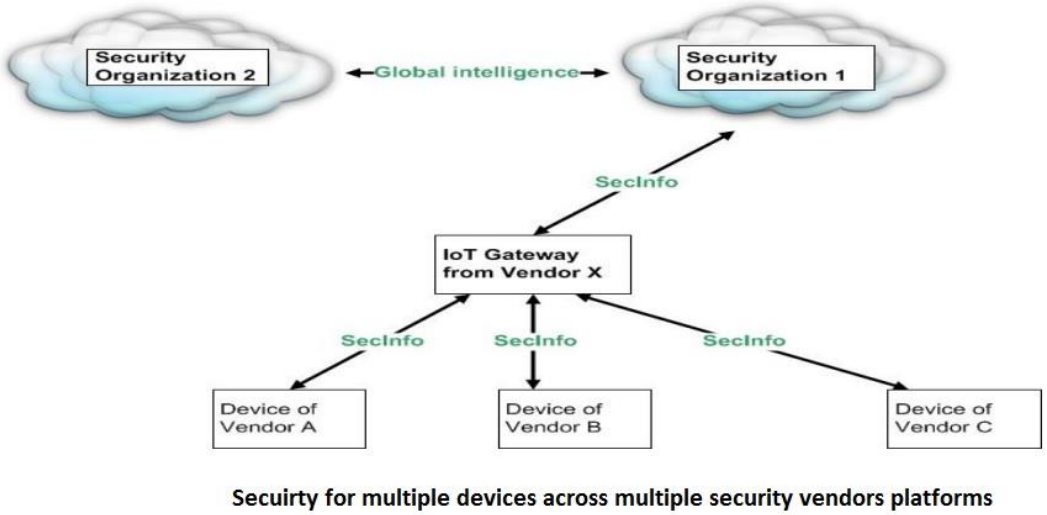


Figure 20: Security of Multiple security vendors (Cross Domain) platforms, courtesy WWRF Template

Cross-certification trust model

- Each organization must individually certify that every other participating organization is worthy of its trust.
- The organizations review each other's processes and standards and their due diligence efforts determine whether the other organizations meet or exceed their own standards.
- Once this verification and certification process is complete the organizations can then begin to trust other organizations users.
- The issue with cross-certification trust model is that when the number of participating cloud grows, the numbers of trust relationships grows also.

Some more models of Trust

- In trust we can consider QoS, key management systems, lightweight PKI certification concept and decentralized system for establishing the trust, which must be alternative to PKI.
- For M2M/IoT systems we need novel method to establish trust in people, devices and data beyond the today's reputation scoring systems.

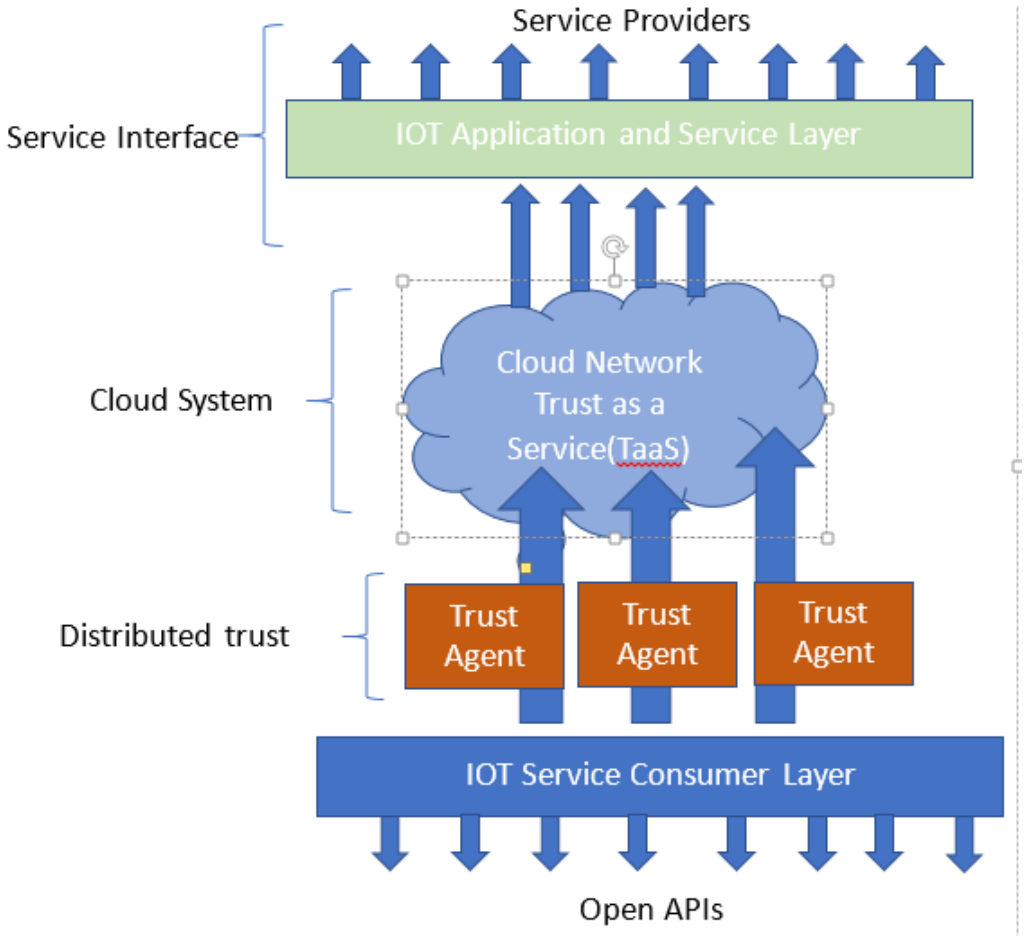


Figure 21: Third-party bridge trust model

- The above diagram (Figure 21) shows the Third-party bridge trust model, in which each of the participating organizations subscribe to the standards and practices of a third party that manages the verification and due diligence process for all participating organizations.

• Once that third party has verified the participating organization, they are automatically considered trustworthy by all the other participants. Later, when a user from a one of the participants attempts to access a resource from another participant, that organization only needs to check that the user has been certified by the trusted third party before access is allowed.

• Trust management in distributed systems like P2P and mobile ad hoc networks is still a big issue. Centralised approach for trust system will be not effective and scalable. The broker framework or third parties trust model are more proper choice for peer to peer networks.

• The idea of the local cloud is to have all things that are required for M2M/IoT environment. This can include many nodes, micro-controllers, embedded devices, smart meters, sensors and actors.

• Everything needs to communicate with the coordinators if there is a mesh network. After coordinators has the local gateway, which can connect to the Internet or to another distributed cloud.

• On the top of the local gateway is running middleware software that is capable to collect the data from sensors and execute M2M applications. It also includes policy module that combine the policy decision and enforcement points in the cloud.

The policies are required when the user want to share the data within the local cloud with other users or to send it to the Internet.

6.5 Sub Group-5: Service Layer Security

Summary of Recommendations of SWG 5: Service Layer Security

Worldwide, the marketplace is witnessing the widespread adoption of IoT/M2M applications in various sectors including the consumer and industrial sectors e.g. Smart homes, Healthcare, Smart Parking, Smart Transportation, Energy Sector and Utilities. Municipalities around the world are also adopting the IoT/M2M, working towards the smart cities that rely on data captured from thousands of diverse sensors spread across a geographic region.

As each vertical industry begins to implement capabilities of the IoT/M2M to meet unique needs and requirements, it will be necessary to evaluate each of these applications for their security weaknesses. Security in these application areas therefore becomes a very important aspect and this document touches upon the vulnerabilities and also the cyber security practices prevalent in the Information Technology sector that are being considered as important in the IoT/M2M sector as well.

However, absence of clear lines of responsibility in the IoT/M2M security makes it a troublesome landscape.

The non-adoption of standards compliant applications and platforms also aggravates this problem and as a result the entire landscape of IoT/M2M remains vulnerable to attacks by the miscreants. As the IoT/M2M and big data continue to transform our personal habits, businesses, and governments, we are left with no choice other than paying more attention and expend more effort in safeguarding both our information and the legitimate systems that make use of it. Standardisation is the only long-term solution towards mitigating this problem in a structured manner.

There is typically a balance between the objectives of functionality and security that must be maintained to ensure that any particular system works correctly, meets business objectives, and is still secure. The same can be said of privacy. While we lay a lot of emphasis on securing the content and the devices, it is also important to ensure privacy of individuals and systems. In the case of the IoT/M2M, it is critically important that trade-offs between functionality, security and privacy be made early on in the design process in order to ensure that all objectives are met equally.

In IoT/M2M, the edge devices play a major role and that is the one which is the most vulnerable as they are mostly in the open and therefore, it is important that at the manufacturing stage itself hardening the

underlying operating system (when applicable), and mitigating hardware-specific vulnerabilities in the platform are taken care of.

In order to handle all the aspects of security and privacy, it is necessary to build it in the core as a service which becomes mandatory for all IoT and M2M applications to follow. In other words, it then boils down to having a common horizontal standard for service delivery which cuts across various verticals while maintaining the uniform philosophy of Security and Privacy.

OneM2M specifications refer to the standard for the Horizontal Common Service Layer for IoT and M2M in which security is one of the Common Service Functions, see Figure 22 below. In oneM2M specifications, Security is dealt with utmost detail without reinventing the wheel i.e. all the established practices which have proven themselves in the Cyber world, are accommodated therein while keeping the door open for the new innovations to be accommodated.

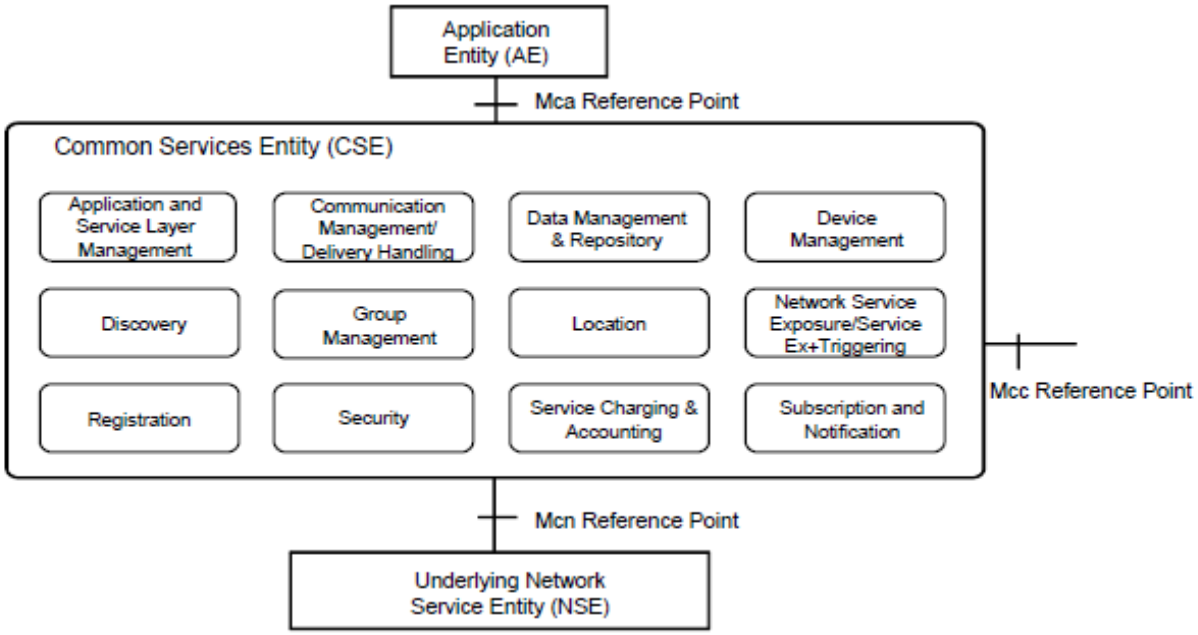


Figure 22: Common Service Functions of OneM2M

7. Recommendations of the Security Workgroup

The Government of India is spending thousands of crores on critical programs such as Smart Cities, Swachh Bharat Mission, Digital India, Make in India which are aimed at readying India for claiming its space in the new world of Industry 4.0, IoT Applications, Artificial Intelligence and Analytics. Deployment of Smart Infrastructure such as Smart Grids, Smart Waste Management, Smart Water, Vehicle Tracking and Surveillance, Remote Asset Management etc. is being targeted to give impetus to this objective, whilst improving the reliability, security and quality of service in everyday life of the stakeholders.

The recent cases such as the use of uncertified Aadhaar Biometric terminals, the Barmer crude oil heist that may have been prevented if the transfer of tracking devices from the truck carrying the crude, to an alternate vehicle had been detected in time, that could not be detected, the Delhi Government (DTC) vs DIMTS centred around the lack of reliability in the service, , the failure of most waste management initiatives to deliver the required impact, have pointed to the fact that much of the Smart infrastructure investment could be wasted if the matters exemplified below are left unattended:

1. Classification of Use Cases and their requirements for Privacy, QoS and Security
2. Registration of Application Service Providers with comprehensive guidelines for Service Capability Declarations and Interoperability
3. Standards, Certification and Compliance procedures for IoT Applications, M2M Communications, Gateways, Devices and Sensors
4. Identity, Authentication and Locking of Devices [e.g. Absence of locking between the SIM card, Device and the Machine, leading to misuse of SIM cards] for the delivery of the required security, safety, manageability, traceability and audit ability aspects of the solution
5. Configuration Control and Remote Management of Devices, Gateways, Connectivity and Subscriptions
6. Improving the assurance of Network Quality of Service especially for use cases classified as sensitive and / or mission critical

Bearing in mind the above, and foregoing sections of this report, the recommendations have been split into two parts

- Recommendations that are (i) Technical Recommendations and (ii) Non-Technical in nature

7.1 Technical Recommendations

The recommendations under this section are a result of assimilating the recommendatory inputs from the various sub-work groups, reviewing individual domain's inputs collectively in the overall context of the IoT / M2M ecosystem including the Devices, Applications, Trust Frameworks, Policy, Regulation, Global Standards, etc. and then focusing the final recommendations to the Indian context.

7.1.1 End to End Security Framework

End to End Security

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.

Remote Manageable and Remote Provisionable

All M2M / IoT Devices and Machines must be remotely identifiable, configurable and provisionable using an Authenticated Channel by the M2M ASP / M2M SP (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.

Security Architecture

The Proposed Security Architecture as given below has been adopted from the various Service Delivery Models described in Section 4.4 [Service Delivery Models] of the TEC Technical Report of Gateway and Architecture.

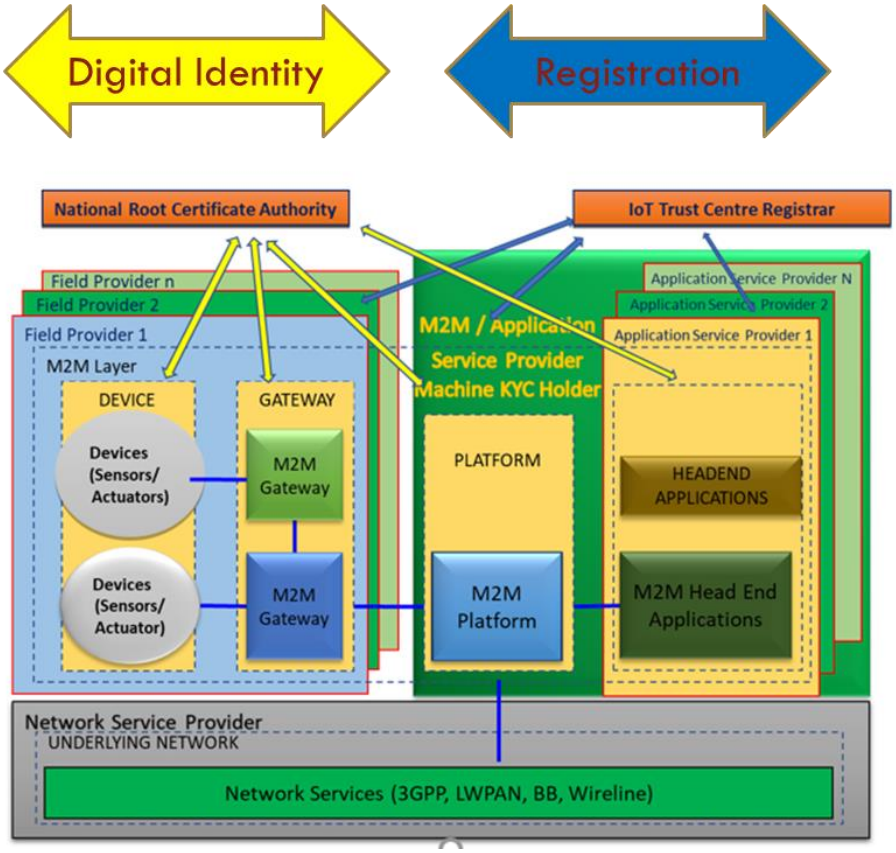


Figure 23: Trust Framework for IoT / M2M, envisioned on the basis of Diagrams of various Business Models identified in the TEC Technical Report "M2M Gateway and Technical Architecture"

Note: The above diagram (Figure 23) has been drawn taking reference from the various Service Delivery Models described in Section 4.4 [Service Delivery Models] of the TEC Technical Report of Gateway and Architecture WG[TEC-TR-S&D-M2M-001-01]. Refer to Figure No 2, Figure No 7-15 of the Report.

7.1.2 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

a. Use Case categories
    i. Mission Critical, High QoS, Sensitive Information [CQS]
    ii. Mission Critical, High QoS, Non Sensitive Information [CQN]
    iii. Non Critical, Best Effort, Sensitive Information [NBS]
    iv. Non Critical, Best Effort, Non Sensitive Information [NBN]
    v. Mission Critical, Best Effort, Sensitive Information [CBS]
    vi. Mission Critical, Best Effort, Non Sensitive Information [CBN]
    vii. Non Critical, High QoS, Sensitive Information [NQS]
    viii. Non Critical, High QoS, Non Sensitive Information [NQN]
b. Mission Critical, High QoS, Sensitive Information [CQS]
    i. All Use Cases serving individual users from governmental or non-governmental infrastructure that affect health, safety or security such as Personal Vehicle Automotive Solutions, Metering Solutions, Home Automation and Safety etc that collect or manage Personally Identifiable Information [PII] or Privacy Protected Information [PPI]
c. Mission Critical, High QoS, non-Sensitive Information [CQN]
    i. All Use Cases serving the public at large from Governmental Infrastructure such as Emergency Services, Disaster Management, Public Safety, Smart Cities, Intelligent Transport Systems, Automotive Solutions, Financial Services (ATMs, PoS, Payment Terminals, Identity Terminals), Health Services (ICDS, Hospital Management) that do not collect or manage information private to individuals
    ii. All Use Cases serving the public at large from non-governmental infrastructure for services such as Emergency Services, Disaster Response, Health Services, Industrial Safety, Transport Services that do not collect or manage information private to individuals
d. Non Critical, Best Effort, Sensitive Information [NBS]
    i. All Use Cases serving a private individual from governmental or non-governmental infrastructure that affect non critical information for day to day use but collect or manage Personally Identifiable Information [PII] or Privacy Protected Information [PPI]
e. Non Critical, Best Effort, non-Sensitive Information [NBN]
    i. All Use Cases serving the public at large from governmental or non-governmental infrastructure that affect non critical information for day to day use that does not in any way collect or manage information private to individuals
f. Other Classifications
    i. Several other combinations of Criticality, Quality of Service and Data Sensitivity are possible which can generate further classifications
    ii. Such classifications may be added in the future, as the need for them becomes evident by use cases that become prominent over time
g. The M2M Service Provider shall register the Application with the correct classification as per classification at (a) above and prominently display this classification on Portals and Apps for the user to be correctly informed

7.1.3 Mandatory Security Compliances for Use Cases

The common minimum requirements of security across all M2M Use Case Classifications is stated (Table 1.) below.

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

Table 1: Common Mandatory Security Requirements

The table 2 below states the mandatory security compliance by Use Case Classification

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		*	

Table 2: Use Case Class Specific Mandatory Security Requirements

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

Certain Use Cases have been examined in greater detail and classified as per the criteria used in Section 7.1.2 above. This illustrative list is appended as Annexure E

In order to assure the security in IOT domain, the mandatory parameters as per table 1 above, namely, Device Identity, IoT/M2M Service Provider Identity, IoT/M2M Application Identity, IoT/M2M Server Identity are essentially required. These can be provided by a National Trust Centre, the framework for which is elaborated in Section 7.2.1.

7.1.4 Security Workgroup Recommendations

In the preceding sections of this report, an effort was made to identify the key components of the IoT / M2M ecosystem, reference security models recommended by Standards and Industry bodies and detail out the threats, challenges and mitigation techniques to keep the IoT / M2M safe.

The diagram below (Figure 24), taken from the GSMA IoT Security Guidelines, is useful to set the context for the security recommendations in this section. In almost all modern IoT service or product models, this diagram defines the primary components that are required when deploying a production-ready technology.

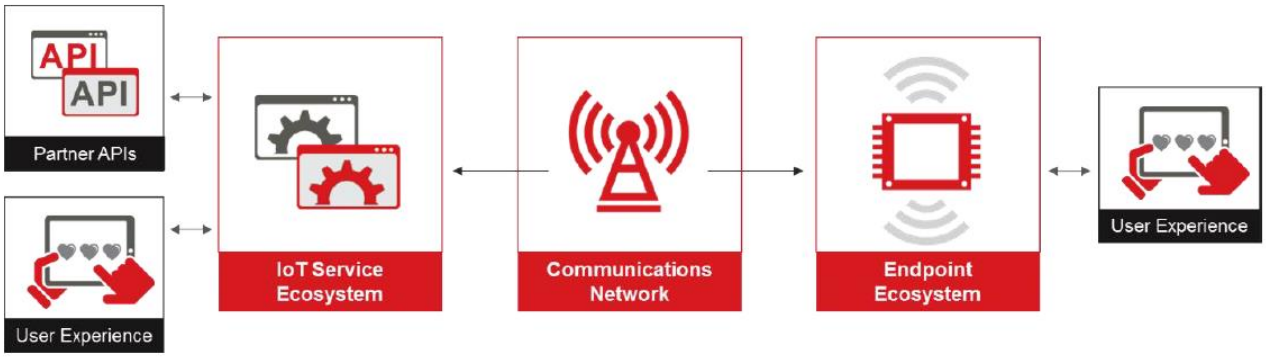


Figure 24: Example IoT Model [GSMA IoT Security Guidelines]

The aspects of Authentication, Authorisation, Encryption and Privacy are expected to be assessed and addressed at various interfaces between the Users of the Device, Users of the M2M Application and the intervening layers of, IoT Services, the underlying Communications Network and End Point Ecosystem.

1. Mutual Authentication

In communications environments, peers speak to each other through the protocol's semblance of identity. An address of some kind identifies the destination of a message. Any communications module that implements a given protocol is capable of stating that it is the owner of a particular address. Unfortunately, most environments are vulnerable to spoofing, meaning that a communication Endpoint's identity can be impersonated regardless of whether the topology traverses a physical or an airwave space. A laptop can change its Ethernet Address, impersonating other computers on a LAN. An IMEI of a mobile device can be changed quite easily.

The protection against this is authentication. For example, in the GSM network, anyone with the right equipment can claim to own any IMSI they choose. However, cellular carriers enforce authentication by encoding a cryptographic key into the Subscriber Identity Module (SIM) that is unique per that subscriber (IMSI). When a GSM device communicates with a base station stating that it is representing a particular IMSI, the base station will issue a cryptographic challenge that can only be solved by someone with the unique cryptographic key stored in the SIM card provisioned for that particular identity. But, even in the case of 2G GSM Networks, it is only the client that is authenticated, not the other way round i.e. an IMSI does not authenticate a Base Station. Newer protocols, such as 3G and LTE, enforce mutual authentication of both entities. This allows Endpoints to cryptographically verify that the base station is serving on behalf of the cellular carrier it claims to serve. However, there are exceptions to this rule too, such as cellular interrogators. The purpose is to establish the idea that communications security is not absolute. It only protects the communication channel between two entities.

For IoT solutions, it is mandatory that mutual authentication is used between the clients and the application server, without relying on the communications channel security. Where it's a peer to peer protocol, each peer in an IoT ecosystem must authenticate all other peers that participate in that ecosystem. The trust model must ensure that proper cryptographic architecture is driving the communications technology, where keys are not easily exposed to adversaries. Once authenticated, each peer must encrypt and sign messages sent to other peers in the network. Each peer that receives a message must cryptographically validate the data prior to acting on it.

2. Authorisation of End Points and Applications

Authorization is the process of granting an authenticated user access to the system resources by checking whether the user has access rights to the system. Authorization procedures enable controls to access rights by granting or denying specific permissions to an authenticated user.

It is essential for M2M Security that trusted end point devices and applications access data in a controlled manner. For this purpose, it is important to control, both, physical and logical access to the end point device and applications.

It is required that M2M Devices and Applications will expose APIs to permit controlled access to the device, application and the data generated by end point devices. Authorisation mechanisms are required to be implemented that restricts access to Devices, Data and Capacity by appropriate control within the Devices, Applications and their APIs.

3. Secure Element

For mission critical use cases, and external secure element is recommended. A Secure Element is recommended for managing digital keys, accelerating crypto processes in terms of digital signings and for providing strong authentication to access critical keys for server applications.

4. Session Layer Security

At the session layer of the OSI (Open Systems Interconnection) stack both SSL (Secure Socket Layer) or TLS (Transport Layer Security) can be used. SSL uses public-key encryption to exchange a session key between the client and the server. This session key is used to encrypt the HTTP transaction. Each transaction uses a different session key. Even if someone manages to decrypt a transaction the session itself is still secure (just the one transaction is violated). In the past encryption made use of a 40-bit (rest of the world) or 128-bit (USA) secret key, but the situation changes as export restrictions are relaxed.

5. Application Layer Security

Application security is really important, for the hacker, it can be considered like an entry point to the system. For that reason a lot of threats and attacks are focused on the application layer. Higher layer security systems have different technology to protect the privacy of the data and applications. Good example for this type of security techniques is PGP. Pretty Good Privacy (PGP) use IDEA encryption, RSA key management and digital signatures. Data integrity is protected by the MD5 algorithm. The internet of things brings both benefits and potential security vulnerabilities. Key steps to securing IoT that enterprises should take to safely connect IoT devices to their networks and improving overall enterprise security.

- Since unsigned software may be compromised, Software release and Software patching must be done in a way that does not compromise the operation of the device. Software updates should only be accepted by authenticated sources to minimize the risk of losing data or interfering with operations

- Access controls are fundamental measures for securing IoT and the organization as a whole. Users and roles assigned should be designated for querying the state of IoT devices, updating software on devices and changing configuration of devices. This can help limit the damage done in the event a user's credentials are compromised.

- Design IoT software analytics with an eye on anomaly detection variation from those baselines can indicate problems. Consider how to respond to anomalous behaviour, perhaps by shutting down problematic devices or removing them from the network to prevent denial-of-service attack.

- Response to anomalous behaviour must be pre-determined, perhaps by shutting down problematic devices or removing them from the network to prevent denial-of-service attack.

6. Privacy

Privacy of End Point data is critical in certain use cases. The principles of informed consent should be enforced for such use cases that are categorised as "Sensitive" as per the definitions within this document.

7.1.5 Domain wise Recommendations

1. Trust Provider and Registration for IoT / M2M domain
    a. It is recommended that 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 issued by DoT on 14th June, 2016, or as modified by DoT / TRAI consultation paper on M2M from time to time.
    b. When registering with the Registration Authority (DoT), the M2MSP / M2MASP should be given a unique identity with a Company Name, Registration_ID, Application_Name, Application_ID, Application_Classification, Start_Date as exemplified below(Figure 25):

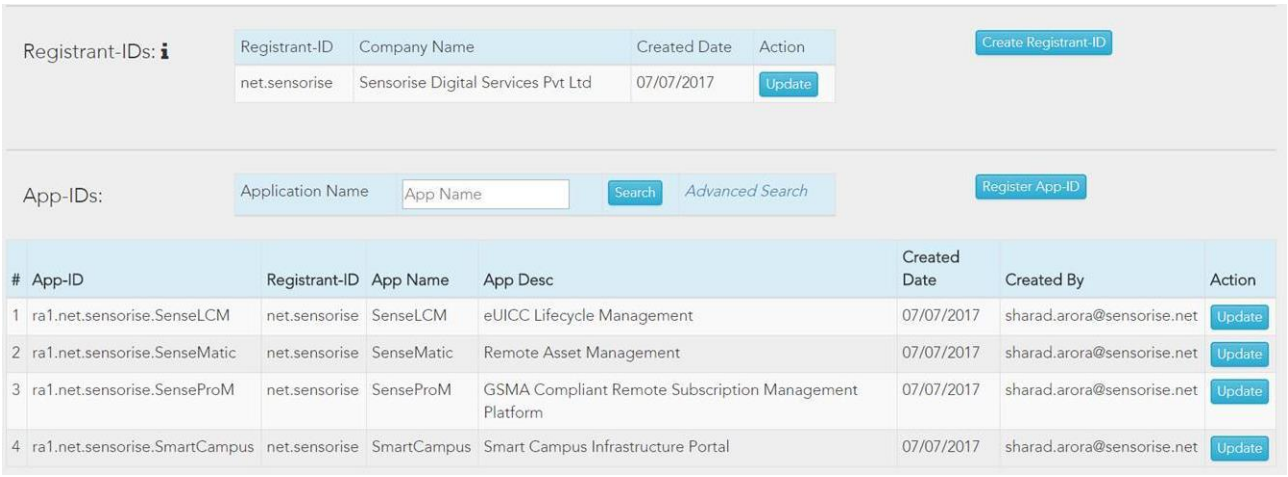


Figure 25: Example of M2M Application Registration

    c. The Hosting of the M2M Service Provider Applications shall be from Cloud or Privately Hosted Servers physically located in India
    d. The 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
    e. There shall be exactly one Server Node per Infrastructure Domain per M2M Service Provider
    f. The M2M Service Provider may have one or more Application Service Nodes, Application Dedicated Nodes, Middle Nodes and Non-one M2M Nodes
    g. The Security Common Services Function hosted by the M2M Service Provider shall ensure implementation of the security functions described below:
        i. Sensitive data handling
        ii. Security administration
        iii. Security association establishment
        iv. Access control including identification, authentication and authorization

v. Identity management

h. The M2M Service Provider that hosts an SMDP and/or SMSR shall ensure its Security Certification from CISA auditor

i. The M2M Application Service Provider shall enable an appropriate Subscription Lifecycle Management capability with which the M2M User can undertake self-care for the fleet of connected devices, either singly or in batches

j. The M2M Application Service Provider shall enable an appropriate Device Management capability with which the M2M User can undertake self-care for the fleet of connected devices, either singly or in batches

k. The M2M Application Service Providers shall be responsible to perform the risk assessment process to identify the specific threats affecting the Use Cases they serve and establish the security needs and the infrastructure required to serve those security needs.

2. Classification and Identification of Devices & Gateways
    a. Devices and Gateways shall be classified along lines of the Use Case classification
    b. All CQS and CQN class Devices and Gateways shall be registered to a M2M Device Registry developed along lines of the GSM Equipment Identity Register with the effect that M2M Service Provider can import a Device or the Gateway at his responsibility
    c. NBS and NBN class devices may or may not be registered to the M2M Device Registry, but the M2M Service Provider shall prominently display / make users aware of the classification.
3. Machine KYC and User KYC

    The concept of Machine KYC has been detailed in the Non Technical Recommendations 7.2.1.2

    a. The M2M Service Provider shall undertake the Machine KYC for CQS and CQN class devices, with the effect that the requirements of the DoT M2M Service Provider Registration shall be fulfilled as below

    "M2MSP shall have ownership of all SIMs taken from Telecom Licensees. The details of all the customers of M2M services i.e. physical custodian of machines fitted with SIMs, shall be maintained by M2MSP. Up-dated information regarding (a) details of M2M end device i.e. IMEI, ESN etc, (b) Make, Model, Registration number etc of the machines (i.e. Cars, Utility Meters, POS etc) corresponding physical custodian's name and address shall be made available online through some web interface to Telecom Licensee and designated Authority by M2MSP. Any changes in customers and machines details shall be updated at the web interface so provided"

    b. For NBN and NBS devices, the M2M Service Provider shall follow the M2M Service Provider Registration and shall allow M2M User to access the device configuration, information exposure and device data to be viewed and downloaded by the User.
4. Classification of Network Services
    a. M2M Devices shall be allowed to use communication services in a technology and license neutral manner
    b. When using the 3GPP technologies, the use of eUICC with multiple profiles shall be mandated for CQS and CQN classified use cases
    c. When using non 3GPP technologies, the eUICC may be used for secure identification and encryption of device data.
5. Data Security
    a. Device Firmware
        i. The M2M Service Provider shall seek from the OEM, and the OEM must provide, a statement regarding the static and dynamic code analysis undertaken for vulnerabilities and penetration tests performed against software to determine vulnerabilities.

ii. The methods for such an analysis shall be guided by industry best practices, an example of which is Open Web Application Security Project (OWASP)

b. Device Data Security
   i. For CQS and NBP class devices [collects, processes or stores PPI] stringent controls will be implemented:
      1. PPS shall state the PPI collected, processed or stored by the device
      2. Provisioning of the device shall require user approval
      3. Data stored on the device should be encrypted using sufficiently strong cryptographic algorithms
      4. Data transmitted from/to the device should be encrypted using sufficiently strong cryptographic algorithms
      5. Access to the device, both physical and logical, should be restricted using appropriate access control mechanisms

c. Application Data Security
   i. Ensuring compliance to DoT / MIETY Guidelines for storage of Data in India
   ii. Ensuring Identification of the Location of Applications, Common Service Layer components and Network Elements
   iii. Handling of Sensitive and PII data, as distinct from other Data
   iv. Data ownership and Retention period must be specified for each Application
   v. Procedures for access to Sensitive / PII when required by Lawful Interception Authorities must be specified
   vi. The Application Data shall be secured as per recommendations of MEITY as applicable to Meghraj cloud initiative from time to time as updated on meity.gov.in

d. Security of Data in transit
   i. The Application Data in transit shall be secured as per recommendations regarding end to end transport layer encryption required for security as per Table 2, Appendix-I and Annexure-E of this report.

6. Quality of Service
   a. 2G networks may be approaching end of life soon, but M2M devices continue to proliferate with 2G Modules. Devices within mission critical and high QoS use cases must use multi-band modules permitting access on 2G / 3G / 4G / 3GPP / Non 3GPP M2M networks
   b. CQS and CQN classified devices must use subscriptions with a Secure Private APN
   c. Use Cases requiring high QoS shall use Multi-access IoT devices, specially within Smart Cities and Smart Infrastructure uses cases
   d. The GSMA eUICC with multiple operator profiles shall be mandated for 3GPP connected devices within CQN and CQS classified Use Cases as also for Use Cases where devices are dispersed, difficult to reach or where the 3GPP coverage is poor
7. Privacy
   a. M2M Service Provider shall conduct a Privacy Impact Assessment (PIA) for the self as per the prevailing laws or as per EU WP29 guidance
   b. M2M Service Providers will have a Privacy Policy Statement based on the PIA that is signed by the Managing Director of the Company. This PPS (Privacy Policy statement) shall be prominently displayed on the website, as part of this practice policy statement, as also submitted annually, or at any change, to the DoT or other such registration authority
   c. M2M Service Providers shall disclose information to the users of IoT/M2M systems about how the data generated from the M2M Devices is planned to be used and acted upon, other than the specific use case in/for which it is generated
   d. The user shall be given an opportunity to opt out of data collection / usage at both, a macro level, and at the most granular level possible
   e. Where the Use Case generates PII or PPI, the application shall always anonymyse the information prior to storing it in repositories in a manner that reverse linkages to the identity of the owner is not possible

f. The duration for which data is stored, and method used for data disposal must be fully described in the PPS

8. Cross Border Subscriptions and Sharing of Application Data
    a. Foreign IMSIs within M2M devices shall be allowed for a period of 3 months, within which time they must be migrated to a domestic subscription
    b. Cross border sharing of Application Data must be done with prior intimation [not permission] to the Department of Telecommunications. The M2M Service Provider must use its judgement and reasonability in protecting national / user interest, and accordingly be liable for action in case of wilful compromise
9. Lawful Intercept
    a. M2M Service Providers shall provide an administrative access to the DoT or other nominated security agencies as directed by the DoT
    b. M2M Service Providers providing location services shall expose an API to the DoT or other nominated security agencies as directed by the DoT, using which the history and recent location data of any device or vehicle can be obtained
10. Inter-operability and Portability
    a. M2M Service Providers shall be required to protect consumers and enterprises by providing and facilitating the migration to other M2M Service Providers in the same domain
    b. The requirement for M2M Applications to trust and inter-operate shall be specified in requirements and standards written per Industry Sector, these are beyond the scope of this document
    c. Procedures for IN-AE to inter-operate with FN-AE between different Service Providers shall be specified in requirements and standards written per Industry Sector, these are beyond the scope of this document
11. Standards
    a. BIS Standards relevant to IoT / M2M shall be applicable to M2M Devices and Applications
    b. AIS Standards shall be applicable to Intelligent Transport Systems, Remote Asset Management Solutions, Public Transport and Surveillance
12. Certification
    a. CQS and CQN classified devices shall be certified by an accredited national or international test and certification labs as per the Standards referred in this Report
    b. M2M Service Provider IN shall be Certified by a CISA auditor
13. Use Cases Map and Security Requirements

Illustration of sample Use Cases and their Classification are given in Appendix-I and Annexure-E.

It is felt that to implement the above recommendations, as exemplified in Figure 23, various IDs such as Device ID, Registration ID, Application ID, Application classifications as well as machine KYC are required, which would require setting up of National Trust Centre, as already recommended by TRAI.

7.2 Non-Technical Recommendations

As explained above, to implement the (security) classification of devices and other recommendations in true spirit, following are recommended by the WG.

7.2.1 National Trust Centre

This Committee is of the opinion that a National Trust Centre be formed under the Umbrella of DoT to implement the various Technical Recommendations as outlined in section 7.1, the Framework of the proposed NTC is as outlined in Section 7.2.1.1.

7.2.1.1 Framework for National Trust Centre

Accordingly, the framework for a National Trust Centre for Connected Objects, relevant to the Indian context of IoT and M2M, is recommended below:

a. Registration of M2M Service Providers
b. Registration of M2M Applications using a Class 2 / Class 3 Certificate taken from the Commercial CA in India
c. M2M ASP interactions coupled through standards based m2m architectures
d. Registration of Devices, which may include following
    i. Record the Embedded Machine Identity or "Machine KYC"
    ii. Identify the Machine's Capability, Configuration and Purpose or Use Case
    iii. Record the Identity [APP ID] of the Application / Server that the Machine is parented to
    iv. 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
    v. Identify the Owner of the Machine with the possibility of admitting changes of the owner
    vi. Command the Machine to reveal its Identity, configuration
    vii. Ensure Location Discovery
    viii. Locking of the Connectivity element to the Remote / Dispersed / Mobile Object
    ix. Ensure Lawful Intercept and Block / Shut Down
e. Remote Provision able Connectivity
f. High Quality of Service in Connectivity meant for mission critical use cases

7.2.1.2 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.

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:

A. Registration of the company offering the M2M Machine / Device / Connectivity with a Trust Authority [e.g. an authorised agency managing the Industry Application such as an RTO, Certificate Provider, Bank, DoT, etc.
B. Registration of the Certified Devices with their IMEI / MAC / Serial Number etc with the Trust Authority from a validated login of the registered OE/OEM
C. Registration of the Connectivity Element, Device and Machine at the database of the agency providing M2M Services, and the export of these identities to the Trust Centre by the agency providing M2M Services using a secure validated access/interface to the Trust Centre
D. Registration of the Custodian of the Machine / Device / Connectivity by the agency providing M2M Services using an OTP to the Aadhaar Linked Mobile Number of the Custodian ensuring an explicit

consent and confirmation from the Custodian of Custodian's Name, Address, Machine Identity, Device Identity, Connectivity Element Identity and the Network Subscription Identity

7.2.1.3 Security Classification for IoT / M2M Devices

At the time of Registration and Certification of Devices, the authorities responsible for Registration / Certification will set out appropriate Test and Certification criteria that enable the Devices to be classified in one of the Classifications mentioned in Sec 6.1.1. This Security classification of Devices shall be clearly visible to the customers as part of Product Data Sheets and the device Manufacturer Practice Statement.

7.2.2 Security Framework

The IoT / M2M Framework must clearly identify the Stake Holders, their Roles, Responsibilities and Mandatory Obligations

Security Framework

Stake Holder	Registrar	Logical Identity / Standards	Digital Identity Association
M2M SP	Competent Authority recommended by DoT	M2M SP ID	Class 2 / Class 3 RCAI Certificate
M2M ASP	Possibility of Registrars by Industry Vertical [ARAI, IMA, MEITY, ISGF etc] It is recommended that a single national registrar, National Trust Centre, is created for all M2M Application Service Providers to provide a uniform layer of administration and compliance	M2M ASP ID	Class 2 / Class 3 RCAI Certificate
Connected Device / Sensor / Gateway Manufacturer Certification	Competent Authority recommended by DoT/ TEC / BIS	As per ANSI / ITU	Embedded Identity as per PAN / 3GPP Standard, Tamper proof and Locked to the Device if removable
Connected Machine	A National Registrar for all M2M Machines that require a Machine KYC	ETSI, GSMA, OneM2M	Tamper resistant linkage between the Machine and the Connectivity Element. Remote Provisionable connectivity and End to End encryption of Data
Remote Management	Identity, Version and Configuration details registered with the Machine KYC holder	AIS-140, OneM2M, TR69, OMA DM	Authenticated Channel for Remote Management using an external Secure Element

In relation to the framework cited above, end to end security means that security associations must be mandated that create a unique and verifiable identification of the Connected Machine, Connected Device, Application and the Service Provider(s) and that a trail of the end to end encrypted transactions are logged and available for interception by LEA Agencies. The use of an underlying transport [3GPP, LPWAN, PANs, LANs, and WANs] layer should remain agnostic to the achievement of the above said objective.

7.2.3 Classification of IoT / M2M Applications / Use Cases

IoT Applications and M2M Communications will touch every aspect of the society, government and industry. It is essential to categorise the Use cases and Applications, and assign to the Categories a minimum requirement for parameters such as Security, Quality of Service, Availability and Privacy as explained above under section 7.1.3

At the time of Registration and Certification of Applications, the authorities responsible for Registration / Certification will set out appropriate Test and Certification criteria that enable the Devices / Applications to be classified in one of the Classifications mentioned in Sec 6.1.1 and Sec 7.1.3. This Security classification of Devices and Applications shall be clearly visible to the customers as part of Product Data Sheets and the M2M SPs Application related Practice Statement.

7.2.4 Specifications, Certification and Compliance for IoT / M2M Devices by Use Case Categories

It is advisable that Certification Requirements for Devices are drafted keeping in mind the different Categories of Use cases and Applications for which they are intended / allowed to be used.

It is essential to ensure that Devices which connect to a network are appropriately certified prior to their introduction to the field as suggested above in section 7.1.5

7.2.5 Enabling Business Model for proliferation of IoT

In order to maximise the Indian innovation and business, the implementation model for rolling out IoT / M2M Services involving M2M SPs / M2M ASPs must be with minimal regulation and an enabling policy, but with maximum care so that the said principles of end to end security are made essential requirements and a pre-requisite for an IoT / M2M service offered to end users to ensure that users' trust and privacy is protected especially in use cases that are in the domain of public services, safety and mission critical infrastructure.

The Department of Telecommunications may register M2M Service Providers, who can take connectivity from any Telecom Service Provider providing connectivity Services in the licensed or unlicensed bands.

The IoT National Application Trust Registrar shall be responsible to register the Applications of M2M Service Providers and M2M Application Service Providers. The M2M Applications shall get their Identities based on Class 2 / Class 3 Certificates issued by a Commercial Certification Authority set up as per the directions of Root Certification Authority of India as per the IT Act 2000.

The M2M SP/M2M ASP [National Trust Centre] shall host the verifiable identity and configuration of all the Certified M2M Devices and Gateways that require a Machine KYC.

The Business Model shall provide for any Indian Company registered to the Indian Companies Act to

- Get Devices Certified as per Essential Requirements framed under Mandatory Testing & Certification of Telecommunications Equipment (MT&CTE) by TEC
- Register as an M2M Service Provider with DoT
- Register the M2M Application or Platform with the National IoT Trust Centre

- Obtain a valid Class 2 / Class 3 Digital Certificate for each of the Application Servers and
- Offer services as per the M2M/IoT Guidelines of the TEC/TRAI/DoT in line with AIS/BIS Standards in the country.

End Points shall store the identity and keys in a non-removable tamper proof area such as a secure element as per 3GPP / ETSI recommendations.

Abstract from Draft DoT M2M Service Provider Guidelines for KYC and Security

> "M2MSP shall have ownership of all SIMs taken from Telecom Licensees. The details of all the customers of M2M services i.e., physical custodian of machines fitted with SIMs, shall be maintained by M2MSP. Up-dated information regarding (a) details of M2M end device i.e. IMEI, ESN etc, (b) Make, Model, Registration number etc of the machines (i.e. Cars, Utility Meters, POS etc) & (c) corresponding physical custodian's name and address shall be made available online through some web interface to Telecom Licensee and designated Authority by M2MSP. Any changes in customers and machines details shall be updated at the web interface so provided."

The recommendations made by the Security Work Group in this report are consistent with the DoT Guidelines and TRAI recommendations.

8. Way forward

The recommendations of the report give rise to a set of potential actions, which may be considered in two parts

- **Further work along lines of the Report, but focused on certain areas of the recommendation that may require a deeper investigation**
    - Prepare detailed guidelines for M2M service provider, including aspects such as Practice Policy Statement (PPS), Privacy Requirements, Data Ownership, Informed Consent, Hosting in India, Tenure of Data Storage, Access for LEAs, Inter-operability and Portability etc. for M2M SP Applications hosted in cloud and data storage servers to be hosted in India
    - For certain focused Ministries / Missions, facilitate discussions on a shortlist of initial use cases for obtaining feedback on the categorisation of uses cases and the implementation of the recommendations in the SWG Report
    - Detailed categorization of all IoT Devices suggesting an allocation of a class of security as defined in the document
    - Prepare an approach paper for the development of the National Trust Centre for registration of M2M devices and applications
    - Study of Last Mile Connectivity options for M2M Devices, addressing issues of security, cost, availability and quality of service
    - Develop an approach paper for Machine KYC, in order to make the custodian verification and machine identification easy and effective
    - The technical implementation of the instructions issued by DOT/TRAI, from time to time, may be deliberated in the future versions of the report as per the future mandate for the Study Group
- **Further actions within the Government, Policy Making and the larger Industry, to benefit the ecosystem with the required security framework**
    - The report to be circulated to the concerned ministries, Standards making bodies and Government ministries/bodies e.g. MEITY, MORTH, MoHUA, MoHA, Ministry of Power, Smart Grid, Smart Cities Mission, Niti Aayog, BIS, etc. to create awareness about the security issues in IoT Projects and invite discussions regarding the potential strategies, approaches and techniques for mitigation of risks
    - Initiate engagements within / by DoT to prepare an Approach Paper for setting up of the National Trust Centre for Devices and Machines.

9. References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

9.1 Normative references

None

9.2 Informative references

The following referenced documents assist the user with regard to the Scope of this document.

[1] oneM2M drafting rules (draft)

[2] TR-0004Definitions and Acronyms

[3] TS-0002Requirements

[4] TS-0001 Functional Architecture (draft)

[5] TR-0001 Use Cases (draft)

[6] ISO/IEC 29115Information technology- Security Techniques – Entity authentication assurance framework

[7] ETSI TS 102 221 V11.0.0 Smart Cards; UICC-Terminal interface; Physical and logical characteristics (Release 11)

[8] ETSI TS 102 671 V9.1.0 Smart Cards; Machine to Machine UICC; Physical and logical characteristics (Release 9)

[9] ISO/IEC 15408: "Information technology - Security techniques - Evaluation criteria for IT security".

[10] ETSI TS 133 220 "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (3GPP TS 33.220)".

[11] ANSI INCITS 359-2004 American National Standard for Information Technology–Role Based Access Control.

[12] NIST Interagency Report 7316 Assessment of Access Control Systems.

[13] DRAFT NIST Special Publication 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations.

[14] OneM2M TS-0003 Security Solutions (draft)

[15] IETF RFC6749: The OAuth 2.0 Authorization Framework, October 2012

[16] TRAI M2M Recommandations, Sep 2017, https://trai.gov.in/sites/default/files/Recommendations_M2M_05092017.pdf

[17] Department of Telecommunications, Gazette NOTIFICATION TESTING AND CERTIFICATION OF TELEGRAPH issued 5th September, 2017

[18] The DoT M2M SIMs, e-SIMs and KYC Guidelines, May 2018, http://www.dot.gov.in/sites/default/files/M2M%20Guidelines.PDF?download=1

[19] The General Data Protection Regulation (GDPR), https://www.eugdpr.org/

[20] ITU-T F.748.1 on IOT Identifier Requirements.

10. Definitions, symbols, abbreviations and acronyms

10.1 Security Related Terms

To enable the average user to appreciate the recommendations in this report, certain Security terms have been explained below.

End to End Security: a service provided by the M2M System to M2M Applications that establishes trusted security credentials to secure connections between applicative entities, independently of other parties involved.

Hardware Security Module (HSM): a separate and tamper resistant physical computing device, , able to perform security procedures related to oneM2M Service functions. The HSM is used within the M2M Device or M2M Gateway and is different from a Server-HSM used within a network infrastructure node / component.

Long-term service-layer key: key used for service-layer relevant security operations. The key is valid permanently or for a significant period of time, i.e. no temporarily derived key material.

Pseudonym: alias identity within the context of the Pseudo anonymity service defined in ISO/IEC 15408 [i9]

Security Mechanism: process (or a device incorporating such a process) that can be used in a system to implement a security service that is provided by or within the system

Security Policy: set of rules and practices that specify or regulate how a system or organization provides security services to protect resources

Security Service: processing or communication capability that is provided by a system to give a specific kind of protection to resources where these resources may reside within the system or any other system

Sensitive Function: function which requires protection from unauthorized monitoring, tampering or execution that is operating on sensitive data / credentials or key material, e.g. derivation of keys from M2M long-term service-layer keys and cryptographic algorithms.

Server-HSM: dedicated computing device, able to perform security procedures related to oneM2M service functions and integrated within M2M network infrastructure servers.

Security Association: a Logical relationship between 2 nodes that are associated with a communication link. Security Associations are not communications links. Security Associations can take a number of forms but in each case they identify the nature of the security service (confidentiality, integrity, authentication or authorisation), the required algorithm and key. Security Associations can be established for single transactions (and thus their establishment can form part of the transaction itself) or for session-based associations (in such instances the association is generally established independently of the individual transactions that are to be secured).

10.2 Symbols

None.

10.3 Abbreviations

None.

10.4 Acronyms

For the purposes of the present document, the abbreviations given in [i.2] and the following apply:

2G	Second Generation
3DES	Triple Data Encryption Standard
3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
AADHAAR	Government of India initiative to offer identity and online authentication to residents
ADN	Application Dedicated Node
ADN-AE	AE which resides in the Application Dedicated Node
AE	Application Entity
AE/CSE	Application Entity/Common Services Entity
AE-ID	Application Entity Identifier
AES	Advanced Encryption Standard
AID	Addressing and Identification
AKA	Authentication and Key Agreement
API	Application Programming Interface
APN	Application Point Name
App-ID	Application Identifier
AS	Application Server
ASM	Application and Service Layer Management
ASM CSF	Application and Service Layer Management CSF
ASN	Application Service Node
ASN/MN	Application Service Node/Mobile Node
ASN-AE	Application Entity that is registered with the CSE at Application Service Node
ASN-CSE	CSE which resides in the Application Service Node
BSF	Bootstrapping Server Function
CA	Certificate Authority
CBN	Critical, Best Effort, Non Sensitive Information
CBS	Critical, Best Effort, Sensitive Information
CQN	Critical, QoS, Non Sensitive Information
CQS	Critical, QoS, Sensitive Information
CSE	Common Service Entity
CSF	Common Service Function
DCF	Device Configuration Function
DDMF	Device Diagnostics and Monitoring Function
DFMF	Device Firmware Management Function
DHCP	Dynamic Host Configuration Protocol
Digital Cert	A digital certificate from a (CA)is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply. An individual wishing to send an encrypted message applies for a digital certificate.
DIS	Discovery
Dla	Interface between Device and Application Layer
DoS	Denial of Service
DM	Device Management

DMG	Device Management Group
DMG CSF	Device Management CSF
DMR	Data Management and Repository
DNS	Domain Name Server
EU WP.29	Working Party 29, representatives of data protection authority of EU Member State
ESN	Electronic Serial Number
ETSI	European telecommunications Standards Institute
ETSI SCP	ETSI Technical Committee Smart Card Platform
eUICC	UICC that hosts one or more Provisioning and Operational Profile(s) with secure over the air selection and changing of subscriptions
FFS	For Further Study
FMEA	Failure Modes Effects Analysis
FN-AE	Field Node – Application Entity
GSMA	Global body coordinating the activities of GSM and its Evolution
GSMA eSIM	eUICC prepared as per GSMA's Embedded SIM Specification providing a single, de-facto standard mechanism for the remote provisioning and management of machine to machine connections, allowing the “over the air” provisioning of initial operator subscription(s), and the subsequent change of subscription(s)
HTML	Hyper Text Markup Language
HSM	Hardware Security Module
HLR	Home Location Register
HSS	Home Subscriber Server
HTTP	HyperText Transfer Protocol
ID	Identifier
IDEA	International Data Encryption Algorithm
IETF	Internet Engineering Task Force
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia System
IMSI	International Mobile Subscriber Identity
IN	Infrastructure Node
IN-AE	Application Entity that is registered with the CSE in the Infrastructure Node
IN-CSE	CSE which resides in the Infrastructure Node
IN-DMG	Infrastructure Node Device Management
IN-DMG-MA	Infrastructure Node Device Management -Management Adapter
IoT	Internet of Things
IP	Internet Protocol
IPE	Interworking Proxy application Entity
ISO	International Organization for Standardization
ITU-T	ITU Telecommunication Standardization Sector
IT ACT	Indian IT Act, together with all its amendments
IoT App	Application for the Internet of Things
LAN	Local Area Network
LPWAN	Low Power Wide Area Network
LDAP	Lightweight Directory Access Protocol
M2M	Machine to Machine Communications
M2M Device	Any M2M End Point or Gateway
M2M Node	Any active device or server capable of hosting an M2M application instance
M2M Network	A network specifically meant or used for M2M communications
M2M SP	M2M Service Provider [M2M Application Service Provider, M2M Solution Provider] as defined in the DoT Guidelines for the M2M KYC and e-SIM
Mca	Reference Point for M2M Communication with AE
Mcc	Reference Point for M2M Communication with CSE
Mcc'	Reference Point for M2M Communication with CSE of different M2M Service Provider

Mch	Reference Point for M2M Communication with external charging server
Mcn	Reference Point for M2M Communication with NSE
MD5	message-digest algorithm 5 for Data Integrity
MEID	Mobile Equipment Identifier
Mla	Interface between Application and Service Capability Layer
Mld	Interface between Gateway and Service Capability Layer
MIP	Mobile IP
MN	Middle Node
MNO	Mobile Network Operator
MN-AE	Application Entity that is registered with the CSE in Middle Node
MN-CSE	CSE which resides in the Middle Node
MSISDN	Mobile Subscriber International Subscriber Directory Number
MTC	Machine Type Communications
MFF2	Solderable Form Factor of the eUICC (SIM Card)
Mobile IoT	Also called Trusted IoT, GSMA Initiative for Low Power Wide Area (LPWA) solutions in licensed spectrum e.g. EC-GSM-IoT, LTE-M, NB-IoT
NA	Network Application
NAF	Network Application Function
NBN	Non Critical, Best Effort, Non Sensitive Information
NBS	Non Critical, Best Effort, Sensitive Information
NQN	Non Critical, QoS, Non Sensitive Information
NQS	Non Critical, QoS, Sensitive Information
NSE	Network Services Entity
OAUTH	Open standard for access delegation
OneM2M	Alliance for Standardisation of M2M / IoT
OS	Operating System
PIA	Privacy Impact Assessment
PII	Personally identifiable information, or sensitive personal information (SPI), is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context
PPI	Privacy Protected Information
PPS	Privacy Practice Statement
QoS	Qualify of Service
Root CA	Certification Authority responsible for enabling and provisioning of trust between CAs
RCAI	Root Certifying Authority of India
REG	Registration
REG CSF	Registration CSF
REST	An Application Programming Interface, is based on representational state transfer (REST) Technology.
RSA	Rivest–Shamir–Adleman Algorithm for Public Key infrastructure
SA	Security Association
SHA	Secure Hash Algorithm
SQL	Structured Query Language
SMDP	Subscription Management Data Preparation
SMSR	Subscription Management Secure Router
TR	Technical Report
TS	Technical Specification
Ua	Interface between NAF and UE
Ub	Interface between BSF and UE
UE	User Equipment
UICC	Universal Integrated Circuit Card
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

URN	Uniform Resource Name
UTRAN	Universal Terrestrial Radio Access Network
UUID	Universally Unique Identifier
WAN	Wide Area Network
WLAN	Wireless Local Area Network
Zh	Interface between HSS and BSF for fetching Authentication information
Zn	Interface between NAF and BSF to fetch the key info over HTTP/Ub interface

Appendix – I Sample use cases and their classifications

The Use Cases examined during the drafting of this report have been presented in the Annexure E, classified according to the security classification and criteria recommended in this report.

The Use Cases are meant to be reviewed in discussion with standards and statutory bodies that belong to the vertical industry with the intent that they are amended or modified as required by the standards / policies applicable to that industry vertical.

In effect, the **Annexure E** is a starting point for a significant next step identified as a way forward after the publication of this report. Which is, the engagement of various important industry verticals that are impacted by the IoT/M2M proliferation to identify the unique requirements of the vertical industry segment and produce further recommendations for those specific use cases.

Annexure – A National Telecom M2M Roadmap

The National Telecom M2M Roadmap, issued by then Minister of MoC&IT in May 2015, highlights the following matters relevant to this report:

"In the future, M2M/ IoT are likely to meld the virtual and physical worlds together in ways that are currently difficult to comprehend. From a security and privacy perspective, the 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. As physical objects in our everyday lives increasingly detect and share observations about us, consumers will likely continue to want privacy. Accordingly, there are security related suggestive guidelines which MSP shall try to incorporate in overall service design to the extent possible as under:

a) To the extent possible, only point to point data, SMS and voices services to predefined numbers only shall be enabled on M2M SIM

b) Enable security of Embedded Sensors to protect from computer worms, viruses or other Malware by implementation of security features like e. g. MILS (Multiple Independent Levels of SECURITY AND SAFETY

c) Additional security in sensors may be incorporated by IMEI & SIM PAIR LOCKING so that sensor shall work with the SIM configured by MSP. However, the reverse is not encouraged i.e. locking by TSP as it will unnecessarily bind MSP with TSP

In order to cater to unique requirements of M2M market, GSMA has recently floated the draft standards of embedded SIM, which tackles security concerns of Telecom operators with respect to ETSI standards of soft or virtual SIMs. In case of Soft SIMs, mobile operator's secret credentials are stored inside the operating system of mobile device whereas in the case of embedded SIM, it embeds existing hardware based UICC into devices and evolves the existing credential distribution mechanism into over the air mechanism. Thus SIM technology is fast evolving and future M2M devices are likely to adopt soft, virtual, embedded SIMs in place of physical SIMs so as to have the ease of remote configuration. Such SIMS should be adopted for M2M devices as it will facilitate change of Telecom Operator at the discretion of customer and will help in meeting KYC norms in case of device transfer, as same SIM can be used across different operators."

Annexure – B M2M Service Provider Registration

Developing identity and trust frameworks to deliver quality, secure and sustainable services is a vital requirement for proliferation of IoT / M2M Services. The few relevant sections of the Draft M2M Service Providers (M2MSP) Registration Guidelines released by the DoT on 14th Jun 2016 are reproduced below:

"M2M Services" means the services offered through a seamless connected network of embedded objects/devices, with identifiers, in which Machine to Machine (M2M) communication without any human intervention is possible using standard and interoperable communication protocols. These includes providing services like Vehicle automation, e-Health, Agriculture automation, Fleet management, Supply chain management OR any other services identified by the Authority from time to time as specified in Annexure I by converging physical infrastructure (e.g. buildings, roads, vehicles, transportation, power plants) and digital infrastructure (IT and Communications infrastructure)

"M2M service providers are likely to have significantly different business and telecom resource utilization model compared to most of the services offered by Other Service Providers. In OSP services, end customer uses his own SIM/ telephone connection to avail services offered like tele-banking etc., whereas in most of the M2M services, individual SIMs or Internet connection is used exclusively for such services i.e. SIM fitted vehicle. In OSP services ownership of SIM normally lies with end user of services, whereas in M2M services, ownership shall be with M2M service Providers in most cases (as explained in subsequent sections). Hence, it would be prudent to have separate category of registration to have oversight over M2M service providers using Telecom resources from authorized TSPs".

"M2MSP shall have ownership of all SIMs taken from Telecom Licensees. The details of all the customers of M2M services i.e., physical custodian of machines fitted with SIMs, shall be maintained by M2MSP. Up-dated information regarding (a) details of M2M end device i.e. IMEI, ESN etc. (b) Make, Model, Registration number etc. of the machines (i.e. Cars, Utility Meters, POS etc.) & (c) corresponding physical custodian's name and address shall be made available online through some web interface to Telecom Licensee and designated Authority by M2MSP. Any changes in customers and machines details shall be updated at the web interface so provided. "

Annexure – C TRAI Guidelines

The honourable TRAI has conducted a nine-month long consultation on “Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications” releasing its recommendations on 5th September, 2017 [http://www.trai.gov.in/notifications/press-release/trai-releases-recommendations-spectrum-roaming-and-qos-related]. The M2M Industry stands to greatly benefit from the honourable TRAI’s recommendations, which has strongly endorsed

The M2M Industry stands to greatly benefit from the honourable TRAI’s recommendations, which has endorsed / recommended the following, amongst many others:

The Role of the M2M Service Provider as envisaged by DoT in “M2M Service Providers Registration –Draft Guidelines June 2016”
That all UL (VNO) holders shall be allowed to provide M2M connectivity as authorized in their existing authorizations. DoT may suitably amend the license conditions of UL (VNO).
In order to facilitate smooth roll out of M2M services utilizing the license exempt spectrum, 1 MHz of spectrum from 867-868 MHz and a chunk of 6 MHz of spectrum at 915-935 MHz is recommended to be delicensed
Connectivity provider using LPWAN technologies operating in unlicensed spectrum should be covered under licensing through a new authorization under UL namely UL (M2M). Such licensees should be allowed to bid for lice1m2d spectrum. The honorable TRAI has also recommended a new license category, UL(M2M), which is presently under deliberations within DoT.
Device manufacturers should be mandated to implement “Security by design” principle in M2M device manufacturing so that end-to-end encryption can be achieved
The Role of the GSMA eUICC (also called the eSIM) for M2M Devices, the use of pre-fitted eUICC for imported devices, with a mandate that ‘Over the air’ (OTA) provisioning of a local subscription is supported
The pursuance of the GSMA guidelines for provisioning of new profile remotely with ‘Over-the-air’ (OTA) mechanism
A proof-of-concept (PoC)/ Pilot testing in integrating the emergency response service on the lines of eCall to make suitable mandatory provisions for emergency communication in vehicles
Permit devices fitted with eUICC in roaming for maximum three years from the date of activation of roaming in the network of Indian TSP and mandatorily converted/ reconfigured into Indian TSP’s SIM within the stipulated period or on change of ownership of the device, whichever is earlier. The Authority/ Licensor shall review the condition later based on the developments and requirements
For imported equipment to which the SIM/ device is fitted with such as automobile/ machines (like earth movers), arms etc. (requiring mandatory registration at local authorities such as RTO, State/ District administration) is transferred/ sold to another party before three years, the roaming device (eUICC) shall also be immediately configured with local subscription/eUICC of Indian TSP. The KYC details of the new owner/ buyer must be compulsorily updated in the database of concerned authorities
It should not be mandatory to use only domestically manufactured SIMs in M2M. Embedded SIMs with standard specifications can be imported and relevant information shall be submitted by importer while import of the devices/SIMs
International roaming in M2M shall be allowed under the well-recognized framework of GSMA ‘M2M Annex’ to keep uniformity of the parameters and processes
In order to boost the M2M/IoT manufacturing in India, the government may consider feasibility of allowing extra-terrestrial usage of IMSI ranges with suitable framework on the basis of country specific bilateral agreements
The Authority understands that in order to promote investment and innovation concurrently in the emerging sector of M2M communications, India needs to have in place balanced and clear rules for data security and privacy. After due deliberation, the Authority will issue comprehensive recommendations on Data Protection.

Annexure – D M2M SIMs / e-SIMs

DoT has issued instructions on 16th May 2018 on M2M SIMs / E-SIMs and the related restrictive practices for bulk issuance and Know Your Customer norms. The Key highlights of the policy are as follows:

- TSPs shall issue M2M SIMs to M2M Service Provider as per the Bulk connection issuance policy
- The M2M SIMs shall have restrictions for Voice Calls to/from ONLY one predefined number, SMS to/from maximum of two predefined numbers, and Data to two predefined IPs
- Voice Calls to Emergency Numbers (Police, Fire, etc) shall not be restricted
- Ownership of all such M2M SIMs issued by the TSP shall be with the M2M Service Provider
- The User of the M2M Machine, Device and Connection [Custodian] shall be verified by the M2M Service Provider as per the norms and published online. In case of a change or transfer of the User, M2M Service Provider will undertake a fresh Custodian Verification and update the records in its database
- The e-SIM shall be allowed in single or multi profile, with over the air remote management
- In order to avoid TSP lock-in, TSPs shall facilitate profile updating Over-The-Air for all use case scenarios of e-SIM
- The TSP must ensure the Lawful Intercept and Monitoring of the M2M SIM

Annexure – E Illustrative Use Cases and Their Security Classification

Ser No	Use Case	Use Case Type	Availability / QoS	Authentication Level	Encryption		KYC		Device					Application			
					End to End	Transport Layer	Machine	User	Identity	Certification	Locking with SIM	Application Authorization	Management	M2M SP ID	Application ID	Server ID	Example of Practice Statement (The App is Used for)
1	**Automotive (Private Vehcle)**	CQS	High	5	Required	Required	Required	Required	ANSI 41	TEC Certified	Required	Required	Real time AT for ID & Configuration	DoT Provided	NTS Provided	M2M SP Defined & Informed to NTS	Tracking the vehicle's location, providing its health parameters & enables infotainment for the passengers.
2	**Transport**																
a	Ambulances	CQS	High	5	Required	Required	Required	Required									Tracking the vehicle's location, providing pateints health parameters & advance information to the hospital.
b	Cargo Integrity Monitoring	CQS	High	5	Required	Required	Required	Required									Tracking the weight of the Cargo, its collection and disposal times.
c	Heavy Containers	CQS	High	5	Required	Required	Required	Required									Tracking transportation of Military Ammunition
d	Heavy Containers	CQN	Medium	3			Required										Tracking transportation of NDMA Relief Material
e	Heavy Containers	CBS	Low	5	Required	Required	Required	Required									Tracking transportation of Power Generation Equipment
f	Heavy Containers	CBN	Low	2			Required										Transportation of Electronic Goods
g	Heavy Containers	NQS	High	4	Required	Required	Required	Required									Transportation of Military Equipment
h	Heavy Containers	NQN	Medium	1													Tracking transportation of Building Material
j	Heavy Containers	NBS	Low	4	Required	Required	Required	Required									Tracking transportation of Gas Cylinders
k	Heavy Containers	NBN	Low	0													Tracking transportation of Garbage
l	Light Commercial Vehcle	NQN	Medium	1													VTS Solutions
m	Nearest bay line	NBN	Low	0													Map and VTS Services
n	Public Transport Tracking and Security	CQS	High	5	Required	Required	Required	Required									VTS Solutions
o	Route Optimization	CQN	Medium	3			Required										Map and VTS Services
p	Ship Yard management	CQS	High	5	Required	Required	Required	Required									Logistics management
k	Vehicle overload	CQN	Medium	3			Required										Map, Transportation, VTS services
3	**Critical Infrastructure**																
a	Agriculture	CQN	Medium	3			Required										Soil nutrient levels measurement and rejuvination
b	Airport	CQS	High	5	Required	Required	Required	Required									Passenger, Cargo, Security management
c	City Digital Map	CQN	Medium	3			Required										Map and route optimization services
d	Flood Monitoring & Control	CQN	Medium	3			Required										Flood Monitoring & Control and asset management
e	Nuclear Plant	CQS	High	5	Required	Required	Required	Required									Nuclear Services management

Ser No	Use Case	Use Case Type	Availability / QoS	Authentication Level	Encryption		KYC		Device					Application			
					End to End	Transport Layer	Machine	User	Identity	Certification	Locking with SIM	Application Authorization	Management	M2M SP ID	Application ID	Server ID	Example of Practice Statement (The App is Used for)
f	Parking vehicle Tickets	NBN	Low	0					ANSI 41	TEC Certified	Required	Required	Real time AT for ID & Configuration	DoT Provided	NTS Provided	M2M SP Defined & Informed to NTS	Vehicle Parking Management
g	Polution Monitoring	NBN	Low	0													Polution Monitoring & optimal utilization of mitigation services
h	Power stations	CQS	High	5	Required	Required	Required	Required									Transformer monitoring, smart grid management
j	Railway Stations	CQS	High	5	Required	Required	Required	Required									Crowd and Logistics Management
k	School safety	CQS	High	5	Required	Required	Required	Required									Security System, Attendance management
l	Smart Parking	NBN	Low	0													Vehicle Parking Management
m	Smart Roads	NBN	Low	0													Traffic Lights / Street Lights management
n	Society vehicle Stickers	NBS	Low	4	Required	Required	Required	Required									Vehicle Parking Management
o	Street/Road Lights	CQS	High	5	Required	Required	Required	Required									Traffic Lights / Street Lights management
p	Traffic Diversion	CQS	High	5	Required	Required	Required	Required									Road congestion management
q	Traffic Light Funtioning	CQS	High	5	Required	Required	Required	Required									Automated traffic management
r	Waste Management	CBN	Low	2			Required										Logistics management coupled with VTS
4	**Healthcare**																
a	Connected Medical devices	CQS	High	5	Required	Required	Required	Required									Real time health management
b	Healthcare Asset management	CQN	Medium	3			Required										Asset management and Disaster response
c	Hospital Digital Map	CQN	Medium	3			Required										Patient management
d	Hospital Hygeine	NBN	Low	0													Campus management and security
e	ICU security	CQS	High	5	Required	Required	Required	Required									Patient, staff and medication management
f	Remote Patient Monitoring system	CQS	High	5	Required	Required	Required	Required									Real time health management and Use based Insurance Services
g	Smart Hospitals	CQS	High	5	Required	Required	Required	Required									Automated pateint care services
5	**Banking and Finance**																
a	Customer Detection	CQS	High	5	Required	Required	Required	Required									Customer que management
b	Emergency alarming system	CQS	High	5	Required	Required	Required	Required									Security System
c	Locker Management	CQS	High	5	Required	Required	Required	Required									Security and access management
d	Realtime ATM monitoring	CQS	High	5	Required	Required	Required	Required									Asset management and Crisis response

Ser No	Use Case	Use Case Type	Availability / QoS	Authentication Level	Encryption		KYC		Device					Application			
					End to End	Transport Layer	Machine	User	Identity	Certification	Locking with SIM	Application Authorization	Management	M2M SP ID	Application ID	Server ID	Example of Practice Statement (The App is Used for)
6	**Building and home Appliances**								ANSI 41	TEC Certified	Required	Required	Real time AT for ID & Configuration	DoT Provided	NTS Provided	M2M SP Defined & Informed to NTS	
a	Connected appliance	NBN	Low	0													Home automation
b	Fire and safety	CQS	High	5	Required	Required	Required	Required									SCADA for homes
c	Light Control	NBN	Low	0													Home automation
d	Security and Access Controls	CQS	High	5	Required	Required	Required	Required									Home automation
e	Smart Thermostate	CQS	High	5	Required	Required	Required	Required									Remote Environment Management
f	Vending Machine Monitoring	NBS	Low	4	Required	Required	Required	Required									Asset management and Crisis response
g	Video Doorbell	NBN	Low	0													Home Security Management
h	Water Treatment	CQS	High	5	Required	Required	Required	Required									City / Society Water management
j	Wireless Lighting	NBN	Low	0													Energy optimization solutions
7	**Travel and Hospitality**																
a	Asset Tracking	CQN	Medium	3			Required										Asset Tracking and optimization
b	Customer Monitoring	NBN	Low	0													Tourism and related services
c	Premises Monitoring	NBN	Low	0													Security Services
d	Supply Chain Monitoring	NBN	Low	0													Supply Chain and logistics management
8	**Smart Retailer**																
a	Connecting customers	CQN	Medium	3			Required										Retail management and targeted advertising
b	Self Help Petrol Pumps	CQS	High	5	Required	Required	Required	Required									Retail management
c	Smart shoping booths	CQN	Medium	3			Required										Retail management
d	Smart Trolly for dedicated billing	CQN	Medium	3			Required										Retail and logistics management
9	**Poultry Farmimg**																
a	Health and well being of cattle	NBN	Low	0													Real time health management and Insurance Services
b	Hygeine Management	NBN	Low	0													Real time health management
10	**Smart Environment**																
a	Air Polution Detection	CQN	Medium	3			Required										Polution Monitoring & optimal utilization of mitigation services
b	Earthquake early detection	CQN	Medium	3			Required										Disater warning and response systems
c	Forest Fire Detection	CQN	Medium	3			Required										Forest Fire Detection and response alarm management
d	Landslide and avalache prevention	CQN	Medium	3			Required										Disater warning and response systems
e	NO2 Sensor for open use	CQN	Medium	3			Required										Environment monitoring and mitigation systems
f	Snow level monitoring	CQN	Medium	3			Required										Avalanche monitoring and warning system
11	**Metering**	CQN	Medium	3			Required										Usage monitoring, alerts and optimization
12	**POS**	CQS	High	5	Required	Required	Required	Required									Usage monitoring, alerts and accounting
13	**All Gateways**																
a	Private	NBS	Low	4	Required	Required	Required	Required									
b	Public	NBS	Low	4	Required	Required	Required	Required									
14	All Biometric Devices	NBS	Low	4	Required	Required	Required	Required									User Authentication

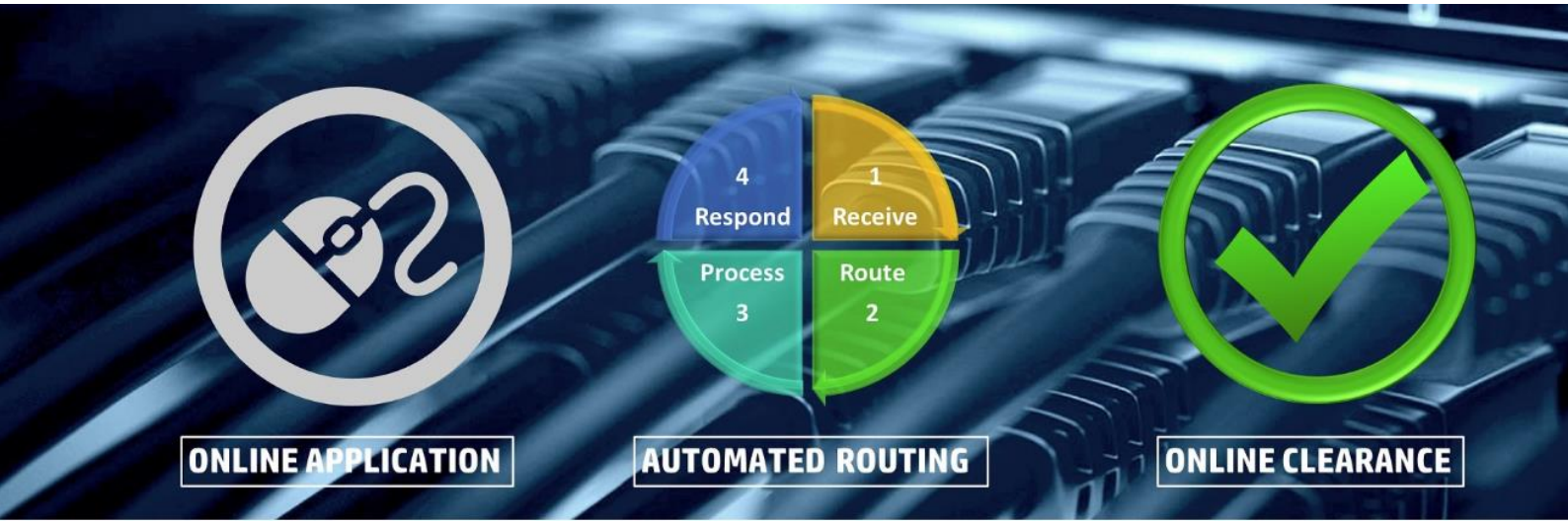
History

Publication history		
V1.0.0	15-May-2017	Draft by SG-3 Lead, circulated for comments to the Sub WG and other Chairs
V 1.0.1	31-May-2017	Addition of a “Core Objectives” Section based on consideration of the scope of other work groups
V 1.0.2	05-Sep-2017	Assimilation of inputs from all sub groups to create a common draft recommendation
V 1.1.0	28-Nov-2017	Draft for Review prior to submission to Sr DGG, TEC
V 1.1.1	13-Jan-2018	Draft for Review after LPCC meeting.
V 1.1.2	16-Feb-2018	Draft for Review after Audio conferencing.
V 1.1.3	27 Feb 2018	Draft for Review after Audio conferencing.
V 1.1.4	15 Mar 2018	Draft for Review after Audio conferencing.
V 1.2.0	28 Mar 2018	Draft for Review after Face to Face (F2F) meeting.
V 1.2.1	25 Apr 2018	Draft for Review after web conferencing.
V 1.2.2	05 May 2018	Draft for Review after web conferencing.
V 1.3.0	20 Jun 2018	Draft for Review after 19-06-2018 web conferencing.
V 1.3.1	26 Jun 2018	Draft for Review after 20-06-2018 web conferencing
V 1.3.2	11 Jul 2018	Draft for Review after 10-07-2018 meeting.
V 1.3.3	14 Jul 2018	Draft for Review after 14-07-2018 meeting.
V 1.3.4	16 Jul 2018	Draft for review after 16-07-2018 meeting.
V1.3.5	21 Aug 2018	Presentation of the Draft Report on 21-08-2018
V1.3.6	30 Aug 2018	Draft for review after 21-08-2018 meeting
V1.3.7	11 Sep 2018	Draft for Review after 7-9-18 F2F meeting
V1.3.8	18 Sep 2018	Draft for Review after in-house LPCC deliberations
V1.3.9	03 Nov 2018	Draft Copy for approval
V1.3.10	1 Jan 2019	Final Copy for approval and print

Sub Groups and Members

S. No.	Name of Sub Group	Members
1	Sub Group-1 End Point Devices Security	1. Mr Pranav Singh / Mr. Vikas Phogat, Idemia (LPCC) 2. Mr. Amit Gupta, Eron Energy 3. Mr. Narang N Kishore, Narnix Technolabs 4. Mr. Sudhir Kamble, TCTS 5. Mr. Mukesh Dhingra, TTSL 6. Mr. Praveen Singh, Eron Energy 7. Mr. Shailendra K Sharma, DDG, TEC 8. Mr. Sanjeev Sharma, Director DOT
2	Sub Group-2 Network Communication Security	1. Mr. Sumit Monga, Unlimit (LPCC) 2. Dr.Debabrata Nayak, Huawei(coordinator) 3. Mr. Vikas Phogat, Idemia 4. Mr. Narang N Kishore, NARNIX Techno Lab 5. Mr. Dinesh Chand Sharma, SESEI 6. Ms. Ranjana Sivaram, TEC 7. Mr. Madhav Chablani, CSA 8. Ms. Divya Sharma, ADG, TEC 9. Mr. Manish Ranjan, ADG, TEC
3	Sub Group-3 Application Level Security	1. Mr. Sharad Arora, Sensorise(LPCC) 2. Mr. SudhirKamble, TCTS 3. Dr.DebabrataNayak, Huawei 4. Mr SumitMonga, Unlimit 5. Dinesh Chandra Sharma, SESEI 6. Mr. MadhavChablani, CSA 7. Ms. Ratna Thakur Director, TEC 8. Dr. S K Samanta, GM BSNL 9. Mr. Manish Ranjan, ADG, TEC
4	Sub Group-4 Trusted Environment	1. Dr. Vijay Madan, TTSL(LPCC) 2. Mr. SudhirKamble, TCTS 3. Dr.DebabrataNayak, Huawei 4. Mr. MukeshDhingra, TTSL 5. Mr. Aurindam Bhattacharya, C-DOT 6. Mr. Shailendra K Sharma, DDG, TEC 7. Mr. VK Arya, DDG TEC (Retd)
5	Sub Group-5 Service Layer	1. Mr. Aurindam Bhattacharya, C-DOT(LPCC) 2. Mr. MadhavChablani, CSA 3. Mr. Dinesh Chandra Sharma, ETSI 4. Mr. Sharad Arora, Sensorise 5. Ms. Ratna Thakur Director, TEC 6. Ms. Divya Sharma, ADG, TEC 7. Mr. Rakesh Kumar, DGM, MTNL 8. Mr. Manish Ranjan, ADG, TEC

Visit us at https://www.mtcte.gov.in



TECHNICAL REPORT

Recommendations for IoT / M2M Security

TEC-TR-SN-M2M-009-01

M2M SECURITY WORK GROUP

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