Enabling the IoT domain with accountable, reliable & future proof M2M connectivity, security by design and interoperable service

Speaker Introduction: Sharad Arora

Engineer by education and profession

Embedded Design Engineer at Xerox

Head of Information Systems at Escotel

Global Management Team member, SmartTrust
Over the Air SIM, Device and App Mgmt Platforms
Root certification Authority in India

Chief Officer, Wireless Solutions at Tata Teleservices
Launched 3G and 3G enabled Solutions
Leader of the Wireless Solutions Sub Committee of Docomo and Tata
Member of the Tata Industries Innovation Council

Founder & MD, Sensorise Digital Services
Credited with the introduction of multi-network solderable SIM in the Indian market place
US Patent "Method and System to control expense & usage of subscriptions in a mobile device"
Stevie Business Award 2019: Most Innovative Telecom Product & Services

Author

- Technical Report on Intelligent Transport Systems, Vehicle to Vehicle Communications and Embedded SIMs (Nov, 2015)
- Author of the ITU Paper on Digital Identity and eKYC for Automotive Industry (Mar 2016, Sep 2017, Jul 2018)
- Lead Author of the Technical Report, Recommendations for M2M Security (Jan, 2019)

Editorial Group, TEC M2M Technical Reports

- Communication Technologies in M2M / IoT (May 2015)
- M2M Gateway & Architecture (May 2015)
- M2M Enablement in Safety & Surveillance System (Nov 2015)
- ICT deployment and strategies for Smart Cities (Jul 2016)

Contributor

- TRAI Consultation on 'Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications
- Member of the MTCTE Committee on Certification
- Member of the Telematics Working Group of Niti Aayog
- Member, Telecom Standards Development Society of India
- Member of National Working Group 13, 17 & 20 aiding the ITU Study Groups
- Rapporteur, Smart Cities Standards Advisory Committee
- Member, 5G Application Layer Standards

Future of World Economy belongs to Apps

5G and IoT Apps need more Security than before

IoT Applications and M2M Communications are exposed to a wider attack surface when compared to the Mobile and the Internet

Other than wireless and mobile, IoT Devices are dispersed

IoT / M2M value chains has several Stakeholders

There is an absence of common standards and certifications

Absence of inter-operability and transferability standards exposes users

IoT use cases are often mission critical

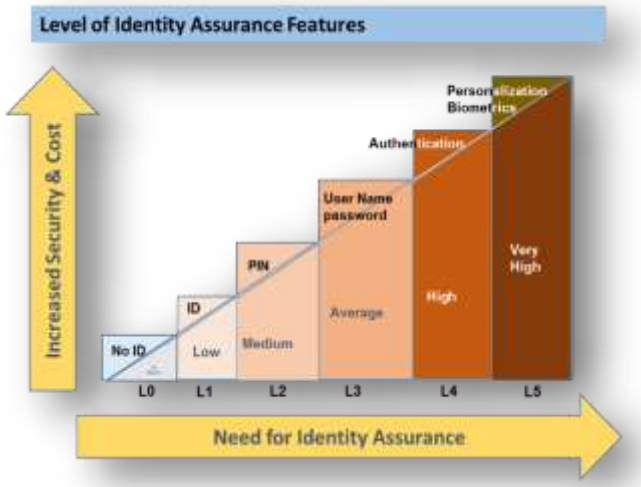
Devices are constrained for resources (Battery, Size, Compute power, etc.)

Price competition exposes the industry to take short cuts

- 5G architecture pushes what was formerly core functionality out to the “edge” of the network
- This has big implications for 5G network security
  - Billions of Devices, Device to Device interactions (relegating the core network to a non-essential element for some types of communications)
  - 200 times 4G bandwidth
- Security concerns
  - potential for unsecure or compromised devices to be used for malicious activity
  - Increases attack surface by orders of magnitude due to software virtualisation and cloud
  - Data explosion leading to difficulty in detecting malicious traffic
  - Major share of global economic output will come to rely on global data networks

Apps need Reliable Connectivity & Trust

Trust and Privacy



Available, Reliable, Resilient, Remote Manageable Connectivity

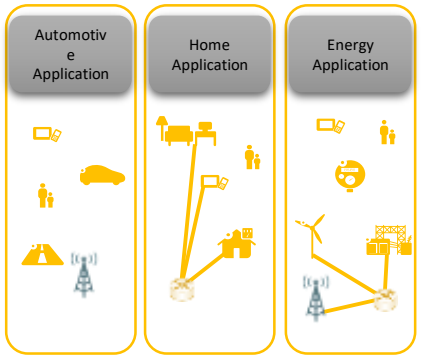
Application Layer Security
- Generic Bootstrap capability
- Device Authentication
- Message Encryption

Network Security
- APN
- Network Layer Encryption
- Secure Messaging

Device Security
- Tamper Proof Identity
- Embedded Secure Element
- Secure Keys & Crypto capability

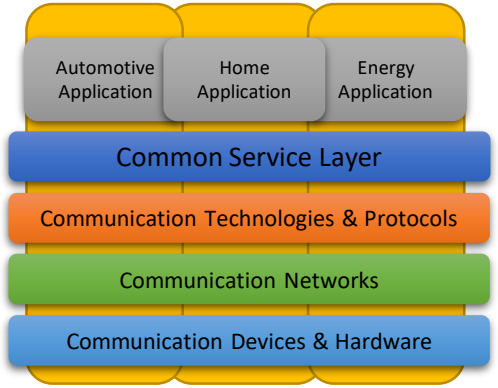
Device Security | Connectivity | Application Security

Guiding OneM2M Reference Architecture



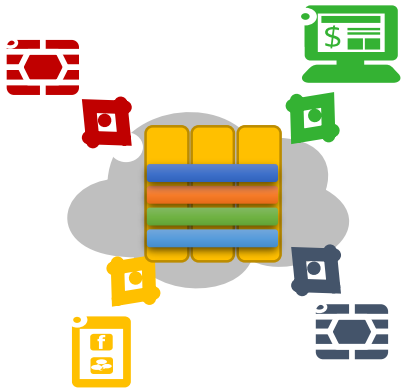
Legacy Solutions are Technology Verticals (Zigbee, DLMS for smart meters, etc.)

Disparate Machines and Applications



Horizontal framework, APIs, Objects as Resource Access Control Policy

OneM2M Common Framework



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

IoT Ready Ecosystem

The Effects on the Ecosystem

(++)

TRAI has recommended an IoT Security Framework based on a

Security by Design and End to End Encryption

National Trust Centre, Registration of M2M Service Providers

TSDSI / DoT / TEC are paving the way for National Standards for IoT

TEC Mandatory Testing and Certification Program for all connected Devices is under way

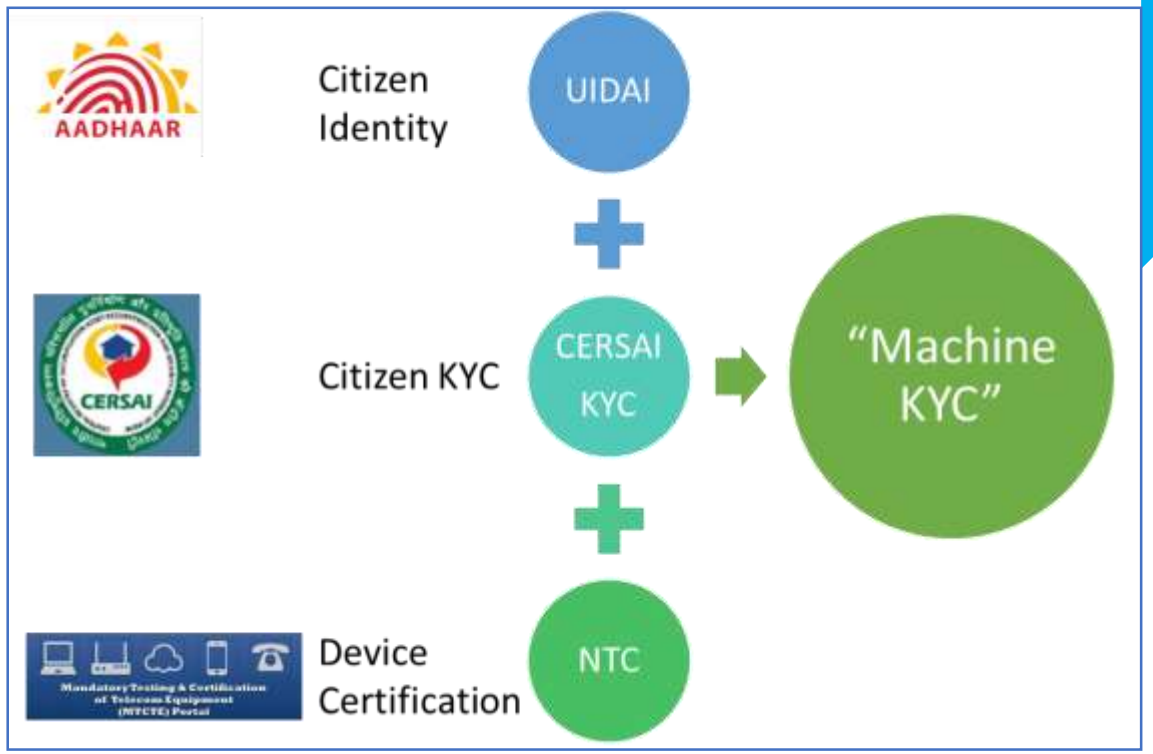
Ministries have initiated deployment of sectoral standards

(-)

Unreliable connectivity has crippled the effectiveness of 1000's of crores invested in the R-APDRP program

Several large SmartCities Projects are feeling the heat from lack of Standards

State wide implementation for tracking services cannot distinguish good devices from rogue devices, plug submission of Data from unidentified sources



New Proposals for Standards | Open Bootstrap Framework

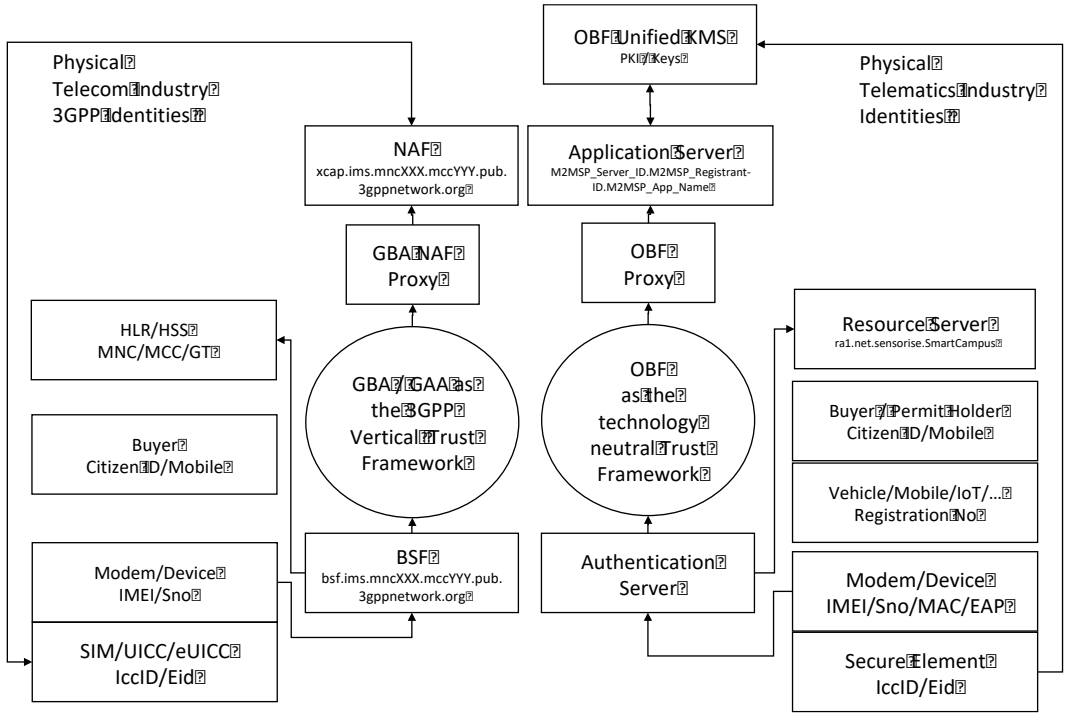
In its current form, the 3GPP GAA Framework is meant for the Mobile network operators (MNO) and 3GPP Network Connected Devices that use the UICC based SIM / USIM / ISIM

A MNO may or may not want to play the role envisaged by the GAA framework. Further, only useful only useful when ALL MNOs offer the framework to allow for seamless changes in subscription during the lifecycle of a connected Device

GAA must become network technology independent

For the global applicability and usefulness of the ETSI GAA, the User / Use Case must be able to benefit from the GAA framework, independent of any one MNO and Network Technologies

The objective of the concept described below is to enhance the 3GPP GAA to be an Open Bootstrap framework that can be MNO and Network Technology independent



THANK YOU