Panel discussion

Topic:

Challenges & Smart Solutions:
Protocol ,Interoperability, Testing and collaboration

People:

1.Mr. Vipin Tyagi -CDOT Moderator
2.Dr. Abhijit Lele BOSCH
3.Mr.Ian Deakin iconnective
4.Mr. Sharad Arora Sensorise
5Mr. Omar Elloumi Nokia
6Mr. Colin Blanchard BT

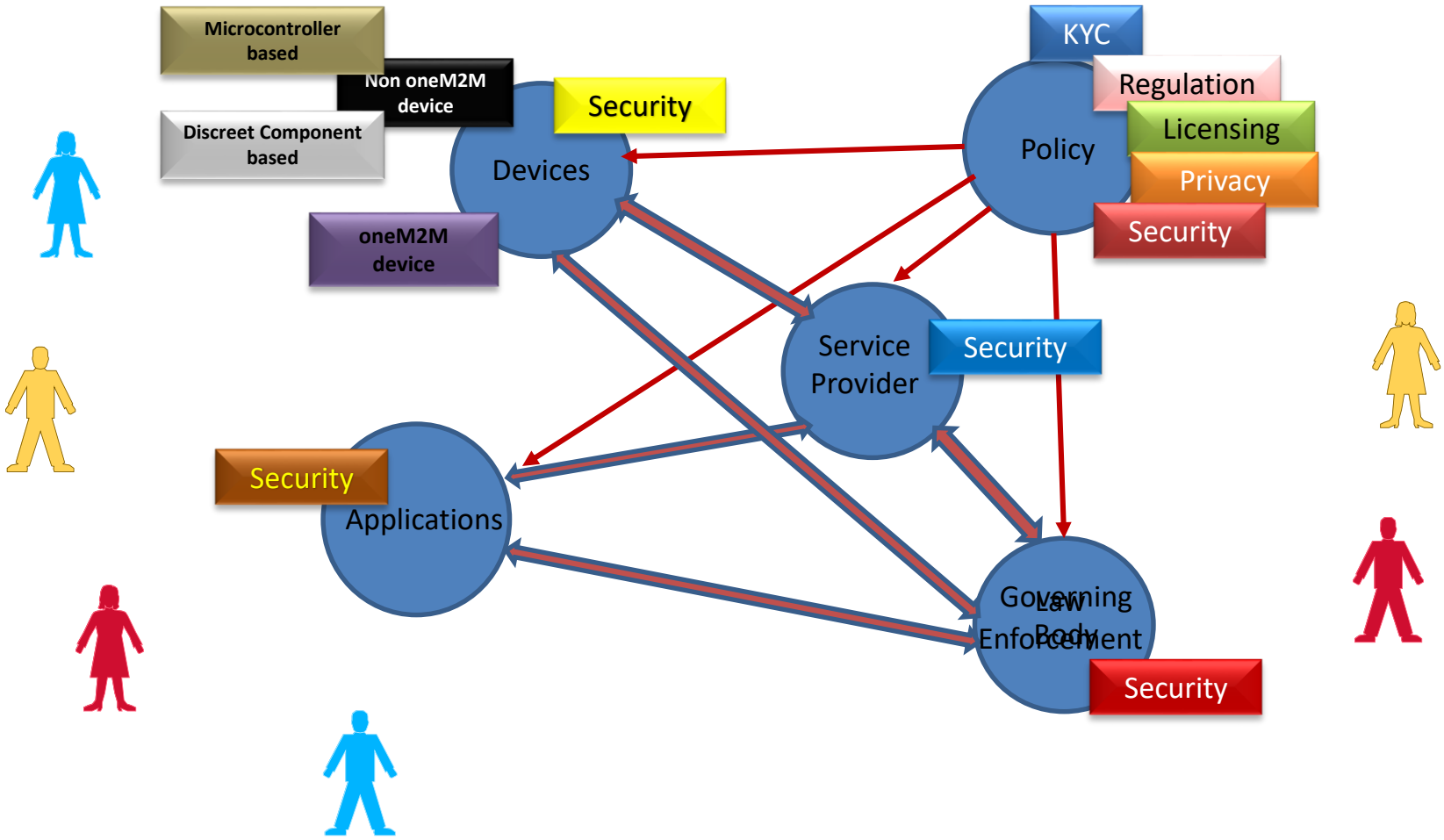
Time

2 minutes introduction +48 minutes/6= 8 minutes per person

Audience:

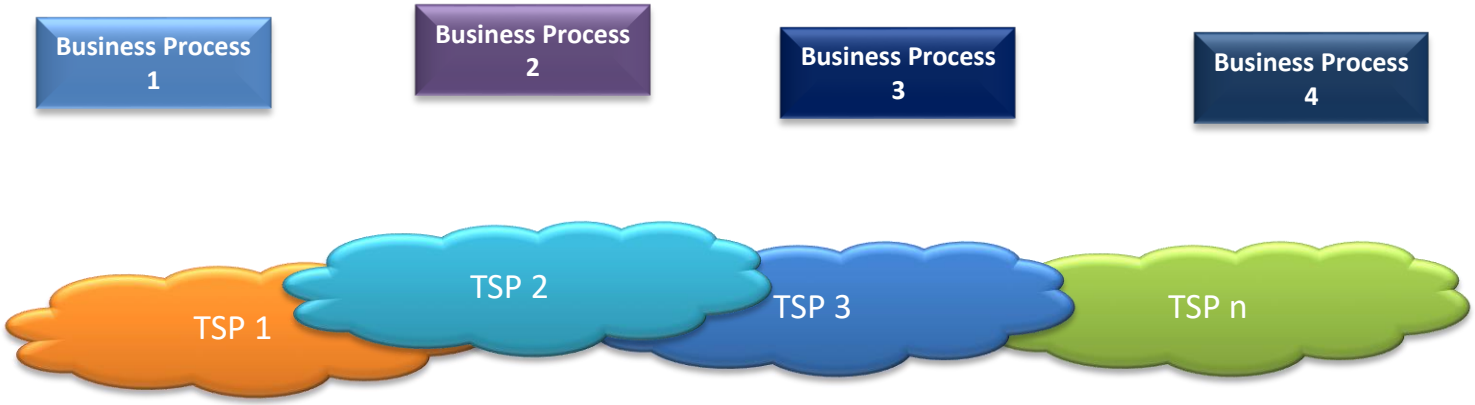
Stay awake ,Clap for Speakers, Note down questions

Actors in the M2M Ecosystem

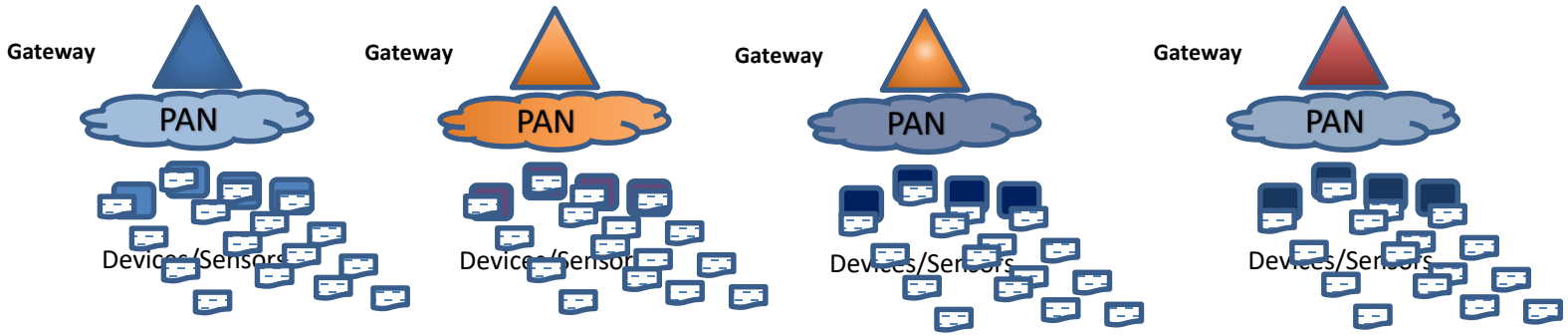


Interoperability - Sharing , Caring, Growing

data being shared between multiple business processes



And there are billions of these devices…!!

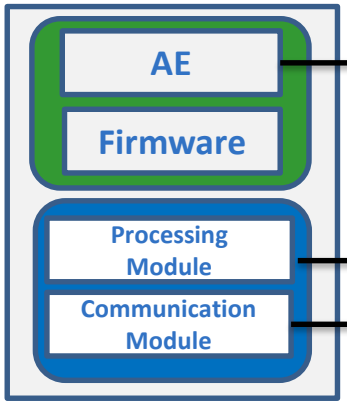


oneM2M Nodes & Functionality

Sensors

Actuators

Non-oneM2M Node (NoDN)

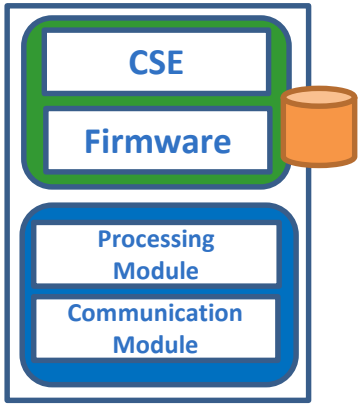


Application Specific

Microcontroller based

Microprocessor based

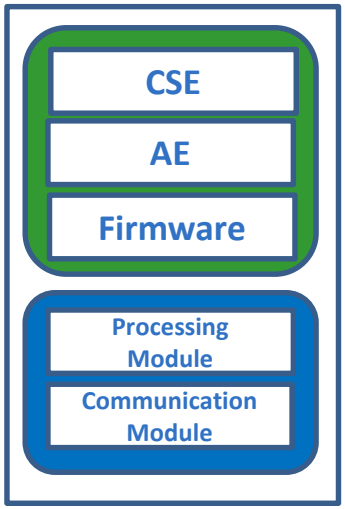
Application Dedicated Node (ADN)



Middle Node (MN)

Infrastructure Node (IN)

Application Server (HES)



Application Service Node (ASN)

Towards Sensor side e.g. LoRa, Zigbee, BLE, Wi-Fi

Towards Infrastructure Domain e.g. Ethernet,3G, 4G etc.

Field Domain

Infrastructure Domain

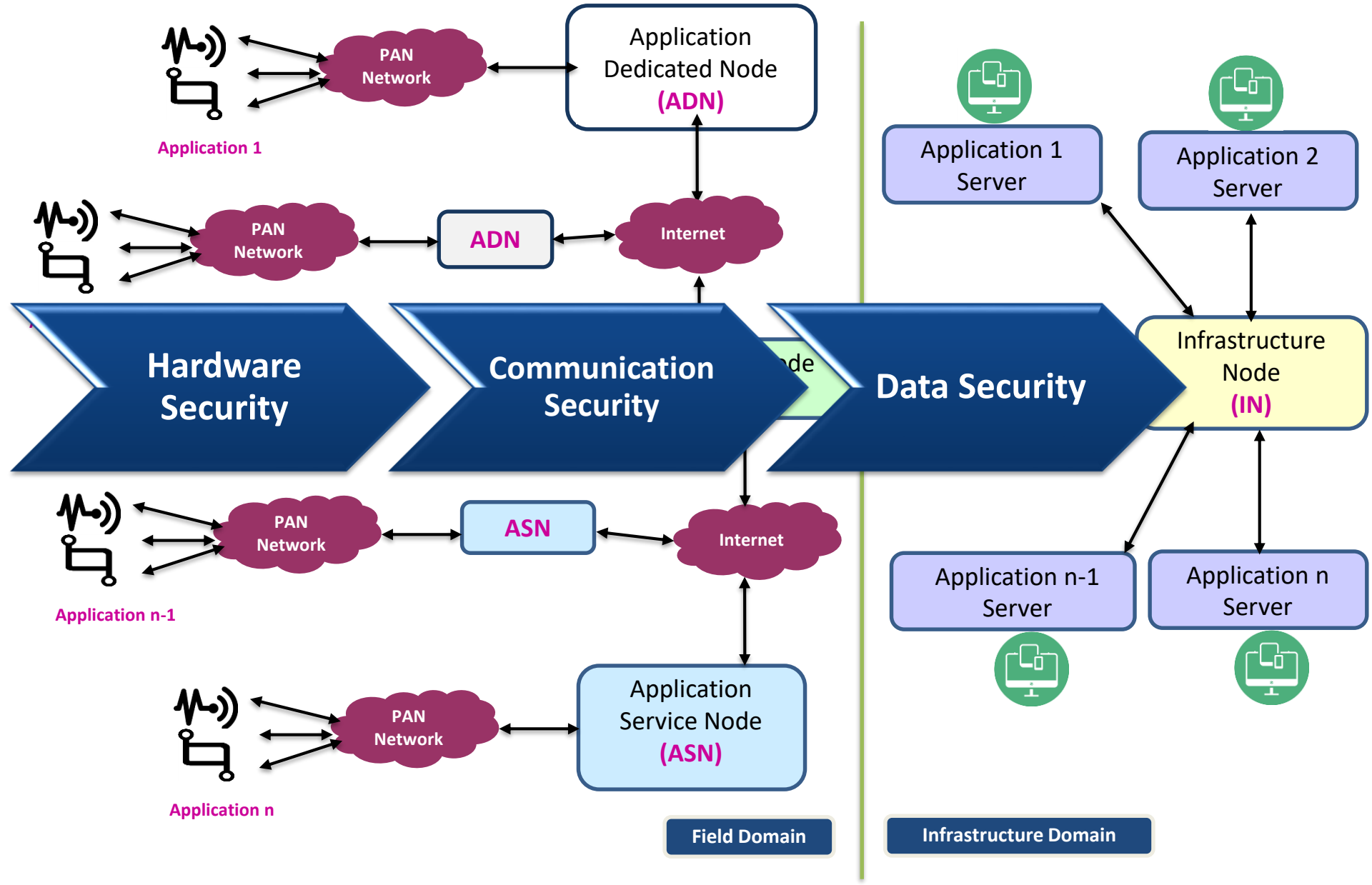
Software

Hardware

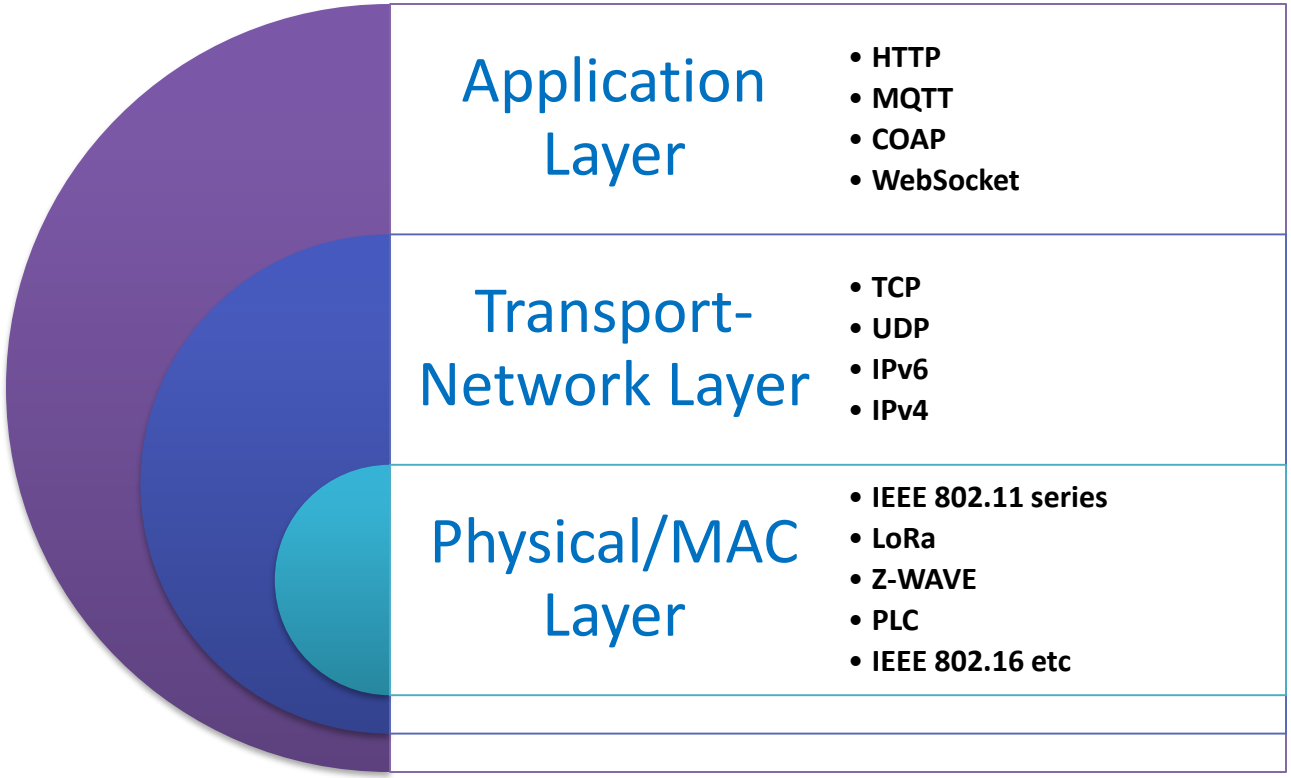
AE-Application Entity

CSE- Common Service Entity

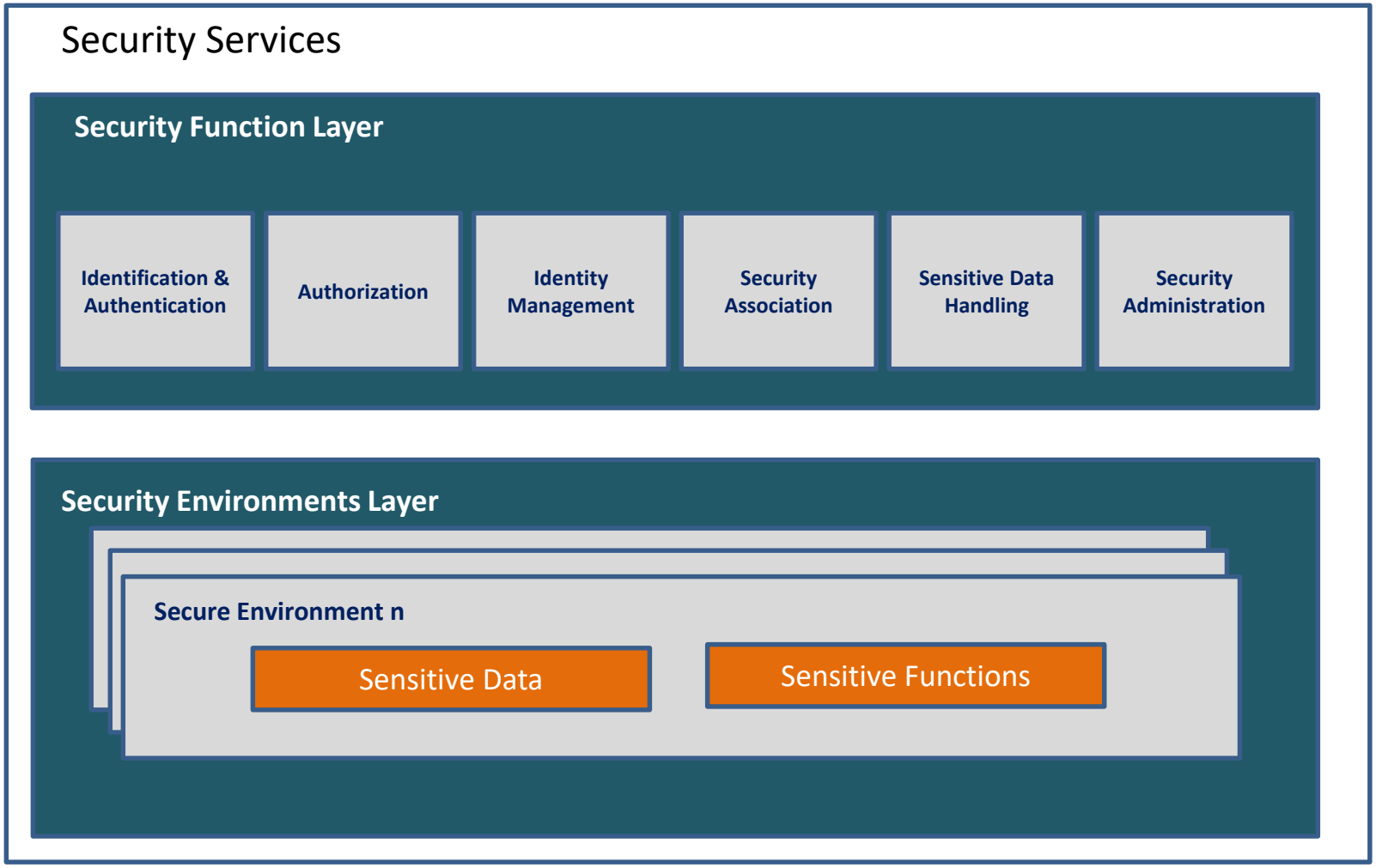
oneM2M Nodes Hierarchy



oneM2M Protocols in different layers

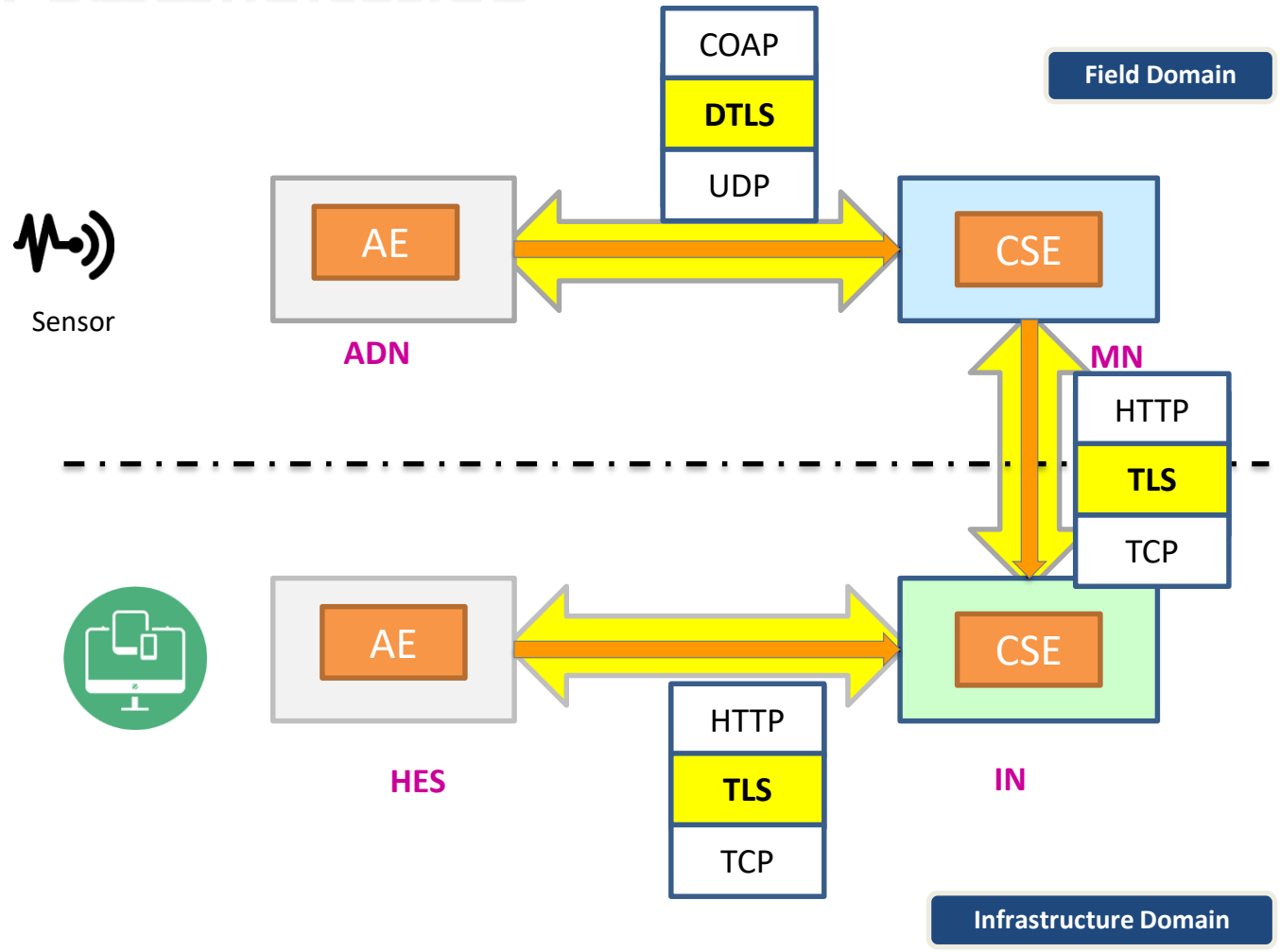


oneM2M Security Architecture



M2M Secure Communication

- Hop-by-Hop
- TLS/DTLS
  - ✓ DTLS if UDP Transport
  - ✓ TLS if TCP transport



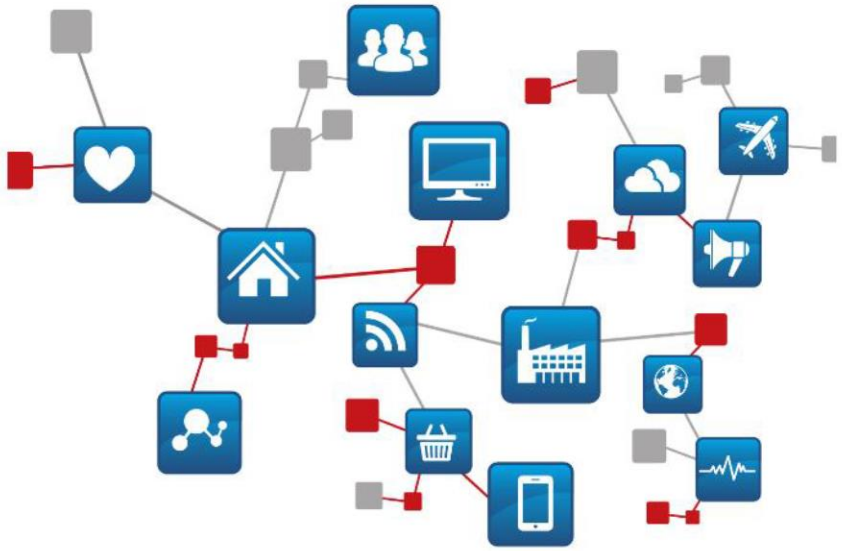
oneM2M Security Measures

Hardware Level Security

- Tamper resistant Storage of long-term Service-Layer Keys within M2M Devices/Gateways
- Non-access to Service-Layer Keys stored within HSM/server-HSM
- Secure Storage of long-term Service-Layer Keys within M2M Infrastructure Equipment
- Secure Execution of sensitive Functions in M2M Devices/M2M Gateways
- Physical/logical Binding of HSM to M2M Device/Gateway

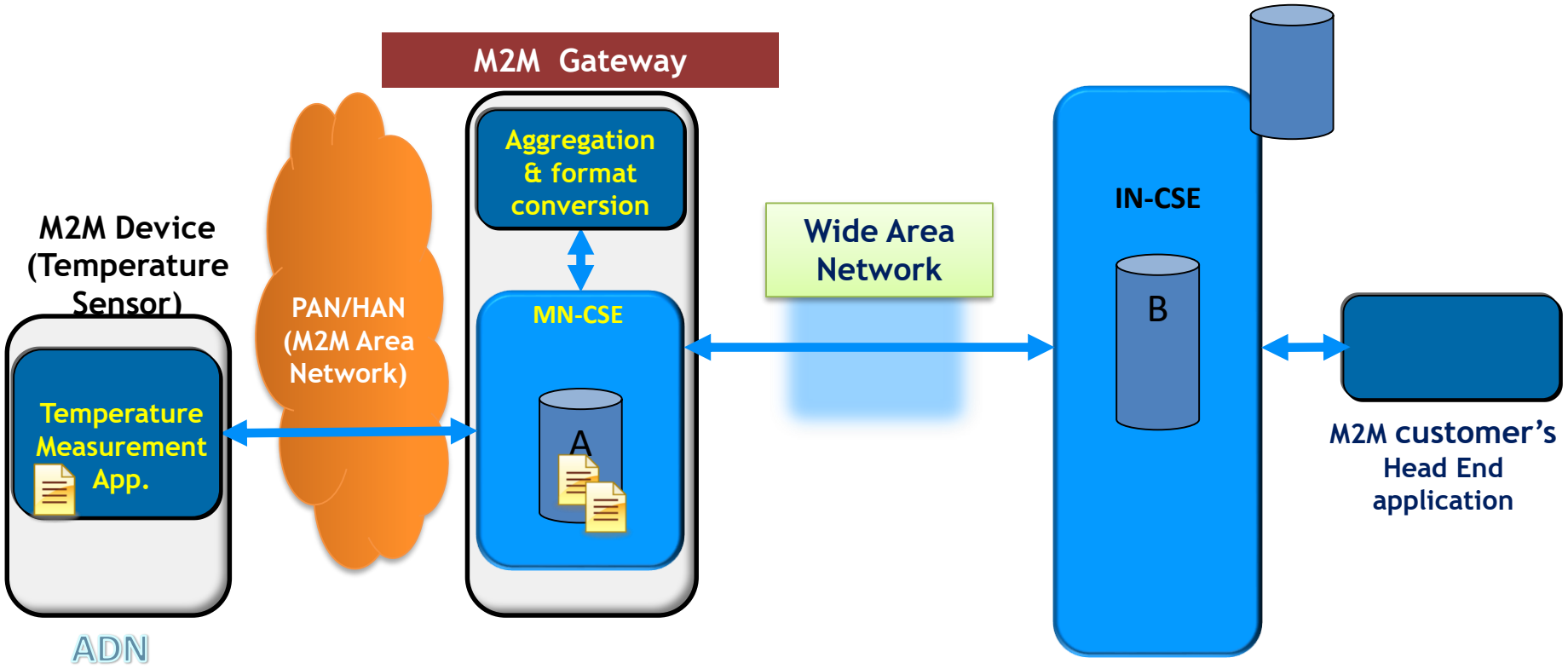
Software Level Security

- Use of Security Associations, mutual Authentication and Confidentiality
- Proven Resistance to Man-in-the-Middle Attacks
- Limited Life Session Keys bound to Service Layer
- Replay Protection along with Policy based Action
- Integrity Verification along with shared Asset Inventory mechanism
- Secure Communication Link with Security Control
- Prevent Injection of Un-trusted Data through parameterized API mechanism



THANK YOU

Real Life Example (e.g. Temperature Monitoring.)



Starting assumptions:
- Bootstrapping / DM is done (provisioning of credentials/apps)
- MN-CSE and IN-CSE have logically connected (authentication, binding, encryption)
- Apps have authenticated to xCSE and access right were established