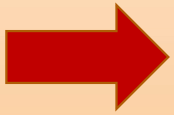
Security, Privacy and Trust in IoT Ecosystem : The oneM2M way

Aurindam Bhattacharya
Scientist G
Centre For Development of Telematics

IoT Threat Assessment

Internet of Computers:

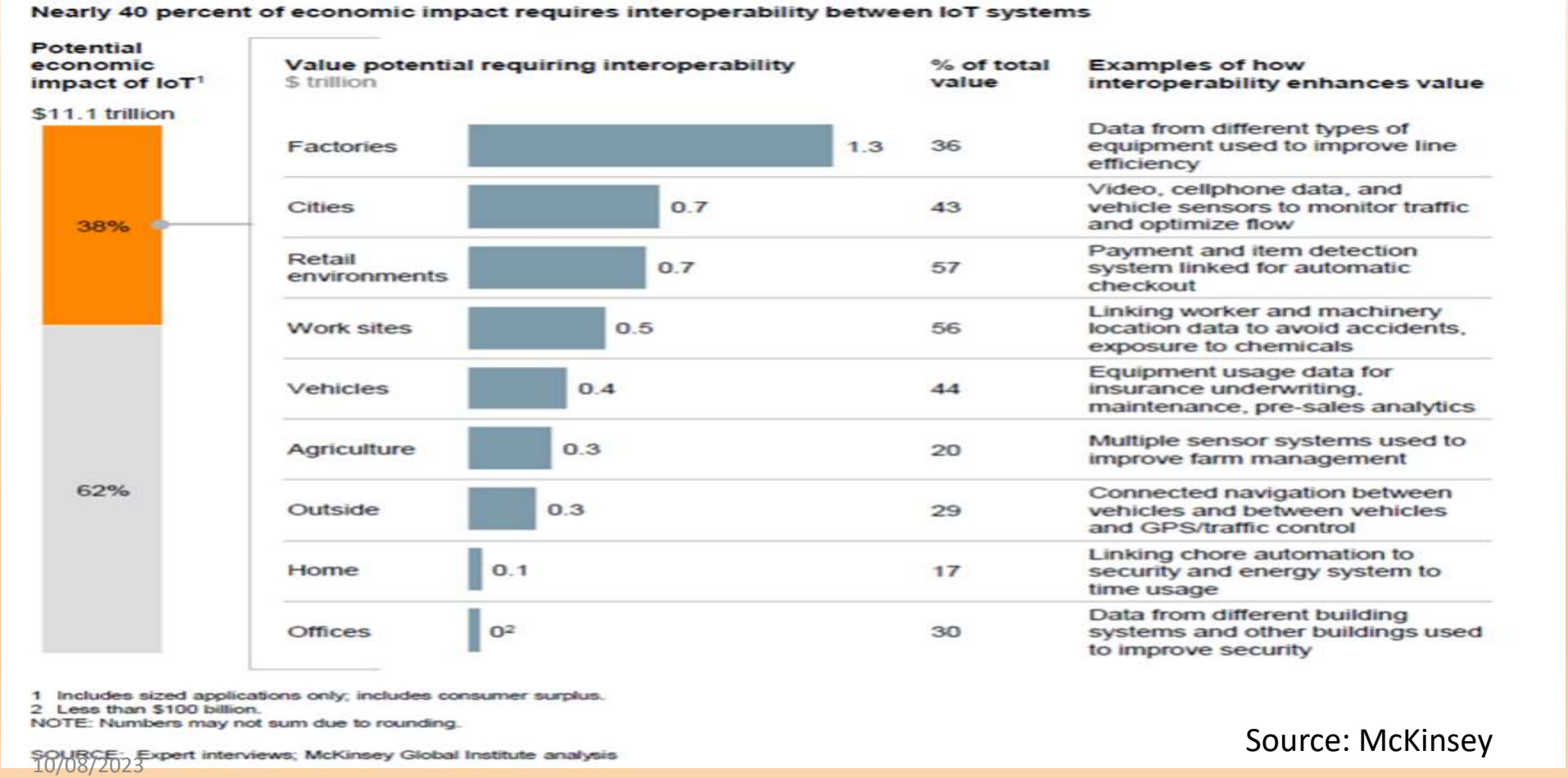
- Attended by human « owners »
- Comfortable, controlled environment
- Relatively fixed location
- Low latency broadband connection
- Few chipsets and OSs to secure
- Few Apps largely deployed
- Rather uniform lifetime
- Relatively powerful resources (computing, memory, energy supply)
- Internet as entry point
- Frequent software security patches
- Ever decreasing cost of attacks
- « Virtual world » impact (information)



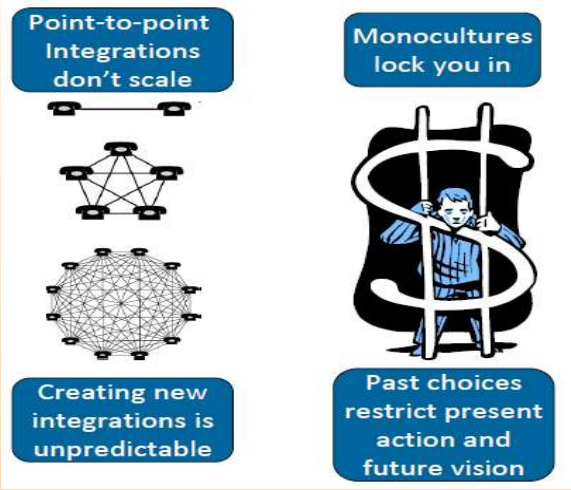
Internet of Things:

- Largely unattended by owners
- Harsh conditions, or physical exposure
- Potentially highly mobile
- Sporadic/constrained throughput/latency
- Diversity of embedded hard and soft
- Multitude of small deployments
- Lifetime from months to decades
- Constrained power, memory, processing
- More, weaker entry points
- Weaker, possibly unmaintained software
- Available and accessible
- Real world impact (physical safety)

40% of economic impact of IoT requires interoperability between IoT systems

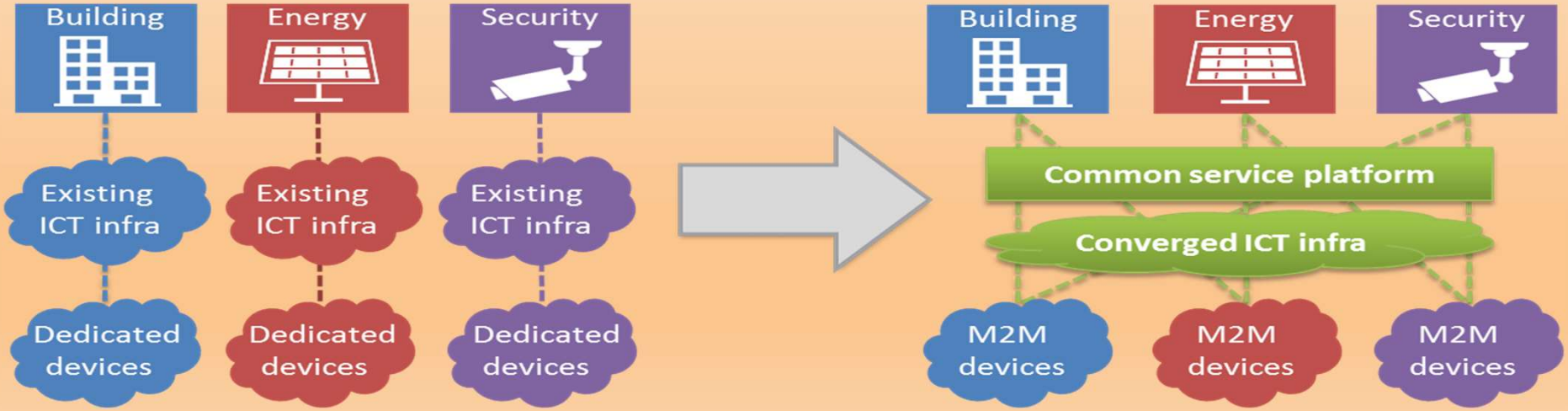


Source: McKinsey



An integrated solution is needed

Highly fragmented market with small vendor-specific or sector-specific solutions.
Reinventing the wheel: Same services developed again and again-
Limited communication and high integration costs



Why use oneM2M?

- THE ONLY STANDARD “DE JURE” DEDICATED TO ENABLE HORIZONTAL IOT INTEGRATION
- DATA MANAGEMENT - DATA HISTORIZATION - INFORMATION SHARING
- VERY DYNAMIC PRIVACY AND ACCESS CONTROL
- SECURE: MULTIPLE SECURITY LEVELS
- STORAGE AND EXPOSURE FOR
  - Historical data
  - Data search and aggregation
  - Context information
  - Dynamic data
  - Real time control and actuation
  - Field device management
  - Network technologies independence
- EASY DB AND CLOUD INTEGRATION
- NATIVE DEVICE MANAGEMENT (DM; TR 069)
- FLEXIBLE IN THE DEPLOYMENT to adapt to the requirements of the various domains
- SCALABLE ARCHITECTURE
- INTER-PROVIDER NATIVE SUPPORT
- DESIGNED BE AN INTERWORKING FRAMEWORK FOR
  - Legacy field and core server technologies
  - Other technologies
  - Proprietary solution

  -> Not an additional solution, but a standard to integrate the different solutions
- SEMANTIC ENABLED TO SHARE INFORMATION
- INTERNET FRIENDLY FOR HUMAN INTERACTION
- SIMPLE if you use the core functions and know your deployment architecture

Opportunities and problems

- **Diversity is the richness** that allows evolution and innovation: combination of services is the biggest opportunity for the future
- But **fragmentation** of solutions and technologies **is the enemy** that is delaying and blocking the developments

- **Simplify** the environment, remove the unnecessary duplicated solutions (economy of scale), **preserve** the necessary/opportune solution specialization by **interworking.**

Opportunities and problems

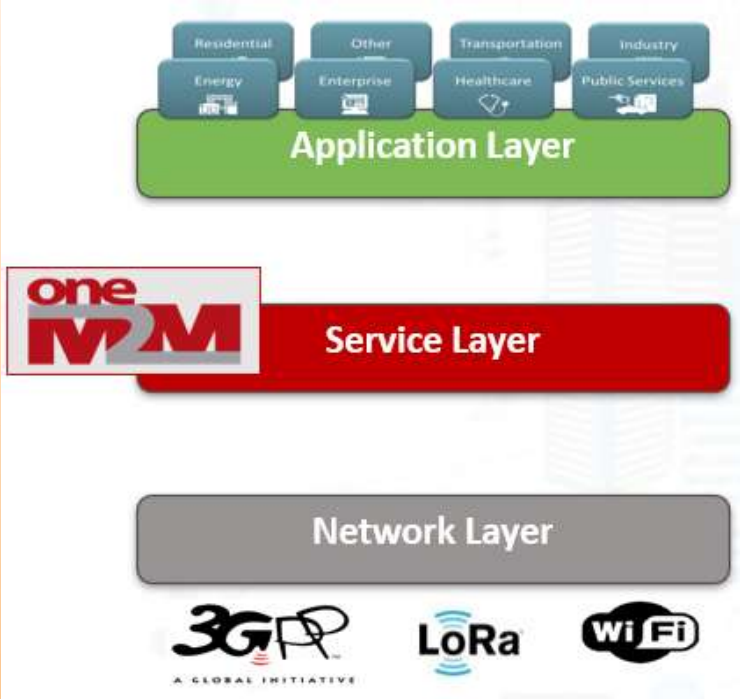
- **Support** the developers community accelerating the development of IoT.
- **Transfer** the competition from integration and platforms to services unlocking the market
- **Reduce** the cost due to the silos approach and its management
- **Enable** Inter-technology and inter-domain data sharing generating new services and new business opportunity

Reduce platform development and integration costs,

enlarge the market,

enable real competition on services

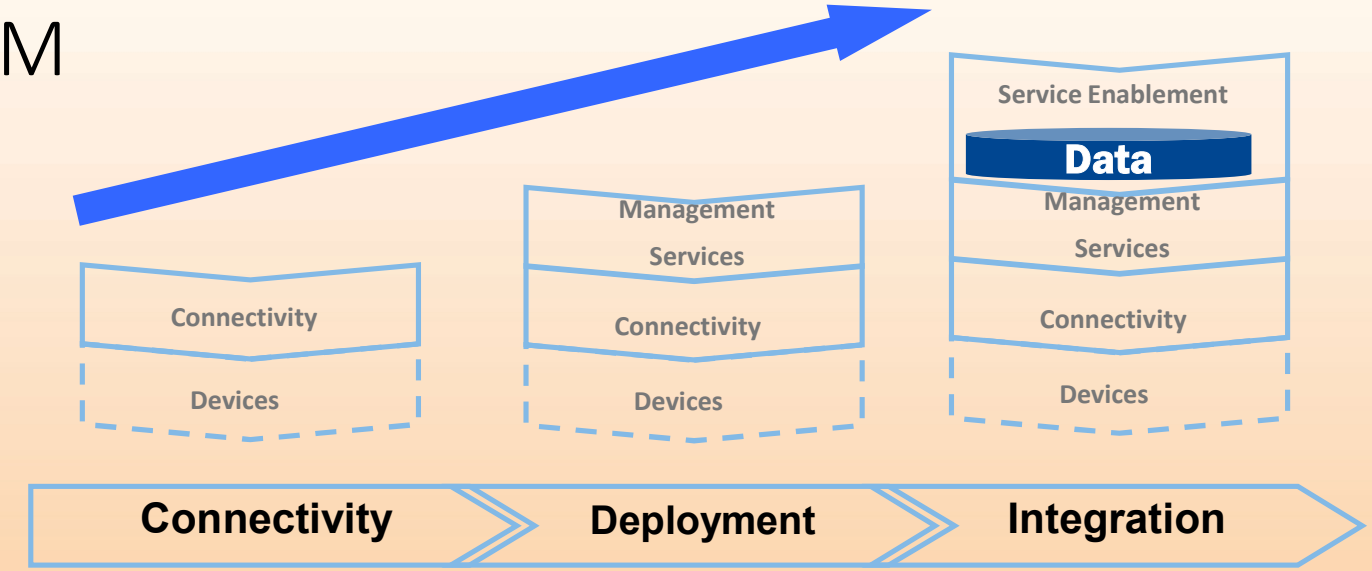
oneM2M



- oneM2M specifies a **distributed software/middleware layer**, sitting between applications and underlying communication networking HW/SW,Integrated into **devices gateways & servers**
- **Bridges** communication technologies, e.g.: **fixed, NB-IoT, 3GPP 4G, 5G, LoRa..**
- **Interworks** existing solutions **(data models)**
- **Manages data** (communicate, store, share)
- Allows to **annotate data** with **semantic descriptions**

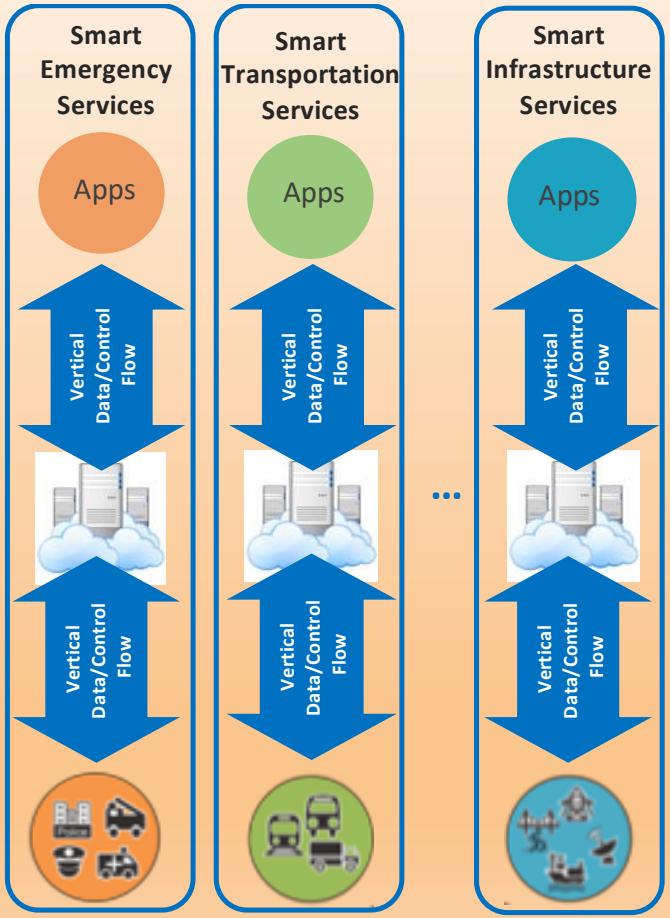
…and most importantly: ***is a Global Standard – not controlled by a single private company!***

OneM2M

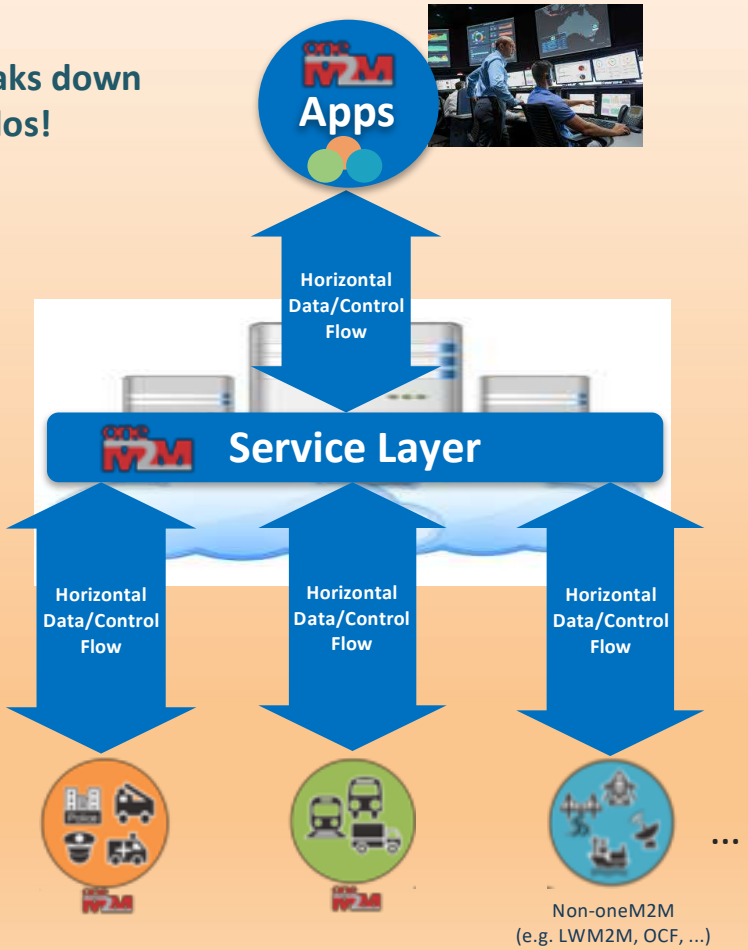


- oneM2M standard is based on a “Store and Share” resource REST based paradigm.
- The data may be made available in the platform to the other applications, interested application are notified by means of subscription
- Privacy is ensured by a strict Access Control Management, which relies on underlying network security, providing a secure light solution
- oneM2M is heavily reusing underlying network functionalities, including TR069 and OMA DM management, LCS, subscription management, QoS, Charging, etc.
- oneM2M is an interworking framewort designed to connect the different IoT technologies

oneM2M integrates the vertical silos!



oneM2M breaks down the vertical silos!



Work flow


Energy
Enterprise
Healthcare
Public Services
Residential
Industry
Transportation
Many others!!!
REQUIREMENTS
TS-0002
TECHNICAL REPORTS
TECHNICAL SPECS

Security in oneM2M Release 2- Release 4

Enrolment services (RSPF / MEF)

Credentials Provisioning/Security Configuration of the M2M System

Secure communications services (SAEF / MAF)

Methods for Securing Information (PSK/PKI/Trusted Party)

Point-to-point and end-to-end solutions (TLS / DTLS)

Access Control & Authorization services

Requester Authentication

Information access Authorization(ACL based)

Static and Dynamic solutions

Privacy Policy Management

oneM2M Secure Environment and security levels

« Secure Environment » concept abstracts the security implementation

- Expose common services to applications, depending on implementation
- Provide common interface for remote security administration, if needed

oneM2M supported implementations distinguish 4 security levels

- No additional security
  - devices otherwise protected from attackers, i.e. on trusted networks
- Software only security (obfuscation, White box crypto etc.)
  - Always vulnerable to sufficiently motivated attacker
  - Acceptable when compromise is not critical
- « Trusted Execution Environment » (TEE) relying on main CPU hardware features
  - Good barrier against software based attacks
  - Sufficient for remotely accessible, but not physically exposed devices
- Tamper resistant hardware embedded Secure Element (eSE)
  - Required to protect secrets within devices physically exposed to attackers (SPA / DPA etc.)
  - E.g. to protect unattended devices against cloning

Summary of Release 2- Release 4 Features

Industrial Domain Enablement

- Time series data management
- Atomic Transactions
- Action Triggering
- Optimized Group Operations

Home Domain Enablement

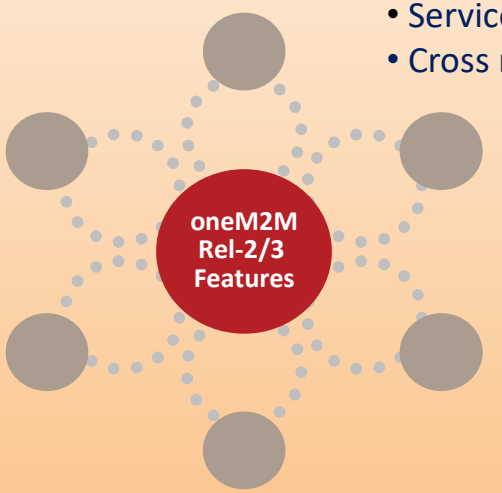
- Home Appliance Information Models & SDT
- Mapping to existing standards (OCF, ECHONET, GoTAPI...)

Smart City & Automotive Enablement

- Service Continuity
- Cross resource subscriptions

Management

- M2M Application & Field Domain Component Configuration



Market Adoption

- Developer Guides
- oneM2M Conformance Test
- Feature Catalogues
- Product Profiles

Semantics

- Semantic Description/Annotation
- Semantic Querying
- Semantic Mashups
- oneM2M Base Ontology

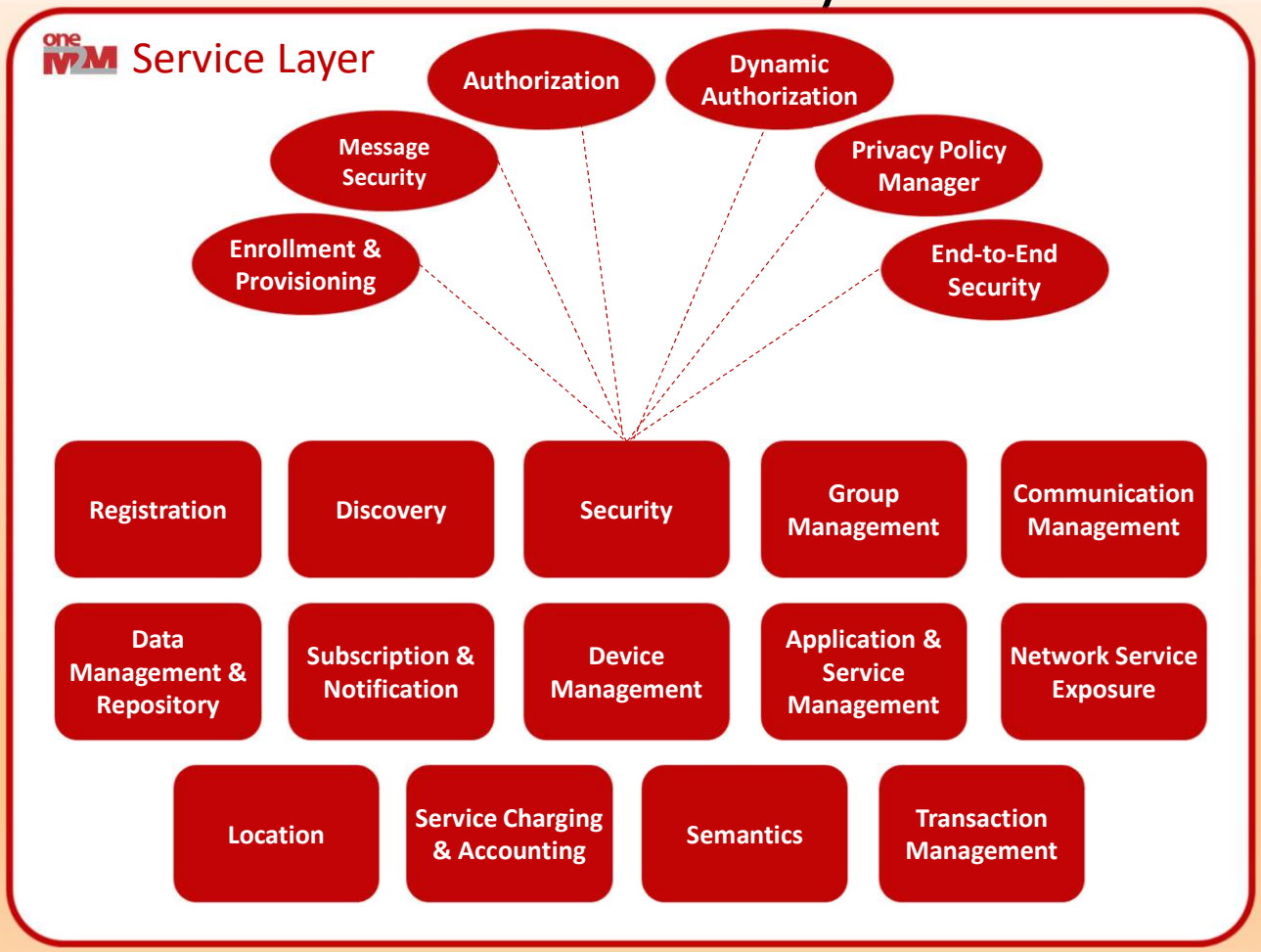
oneM2M as generic interworking framework

- 3GPP SCEF
- OMA LWM2M
- DDS
- OPC-UA
- Modbus
- AllJoyn/OCF
- OSGi
- W3C WoT

Security

- Dynamic Authorization
- End to End Security
- Enrollment & Authentication APIs
- Distributed Authorization
- Decentralized Authentication
- Interoperable Privacy Profiles
- Secure Environment Abstraction

oneM2M Security Framework



- oneM2M provides a common set of security capabilities to secure IoT devices and applications and prevent/ mitigate attacks
- oneM2M exposes an abstracted set of security related APIs to help simplify security for IoT devices and applications

Security in oneM2M Release 2-Release 4

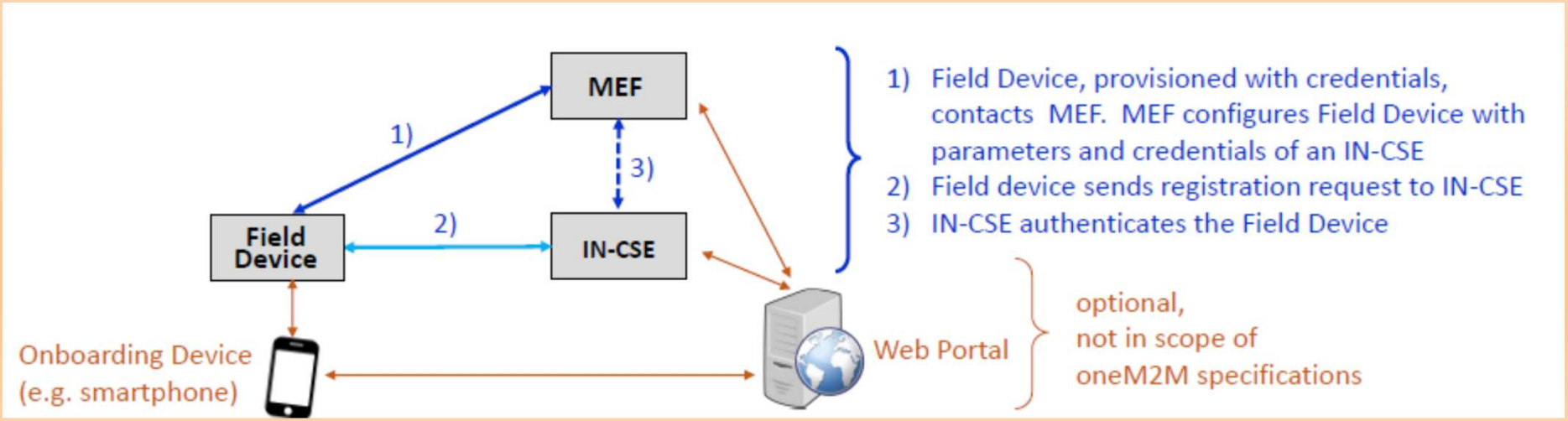
- **Main security functions supported:**
  - Identification and Authentication
    - Identification: checking if the identity of the request originator provided for authentication is valid
    - Authentication: validating if the identity supplied in the identification step is associated with a trustworthy credential
  - Security Association Establishment
    - Establishment of a security context between communicating entities to provide confidentiality (encryption) and integrity
    - Range of authentication options supported
  - Authorization (Access Control)
    - Authorizing services and data access to authenticated entities
  - Remote Provisioning

Security in oneM2M Release 2-Release 4

- **Additional security functions:**
  - Identity protection
    - Capability to use pseudonyms to protect anonymity of transactions
  - Sensitive data handling
    - Capability to protect sensitive data (e.g. local credentials) and functions (e.g. data encryption/decryption) in a Secure Environment (e.g. Smart Card or Virtual Smart Cart)
  - Security administration (related to device management)
    - Creates and administers dedicated Secure Environments and post-provisioning of master credentials

Enrollment & Provisioning (Onboarding)

- Onboarding is the procedure of bringing IoT Field Devices into operation in an IoT network
- Procedures must cope with large variety of field devices types and Service Provider‘s business models
- oneM2M has specified an “M2M Enrolment Function“ (MEF) which enables stakeholders to setup their preferred onboarding and enrollment mechanisms in an interoperable way



Enrollment & Provisioning (Onboarding)

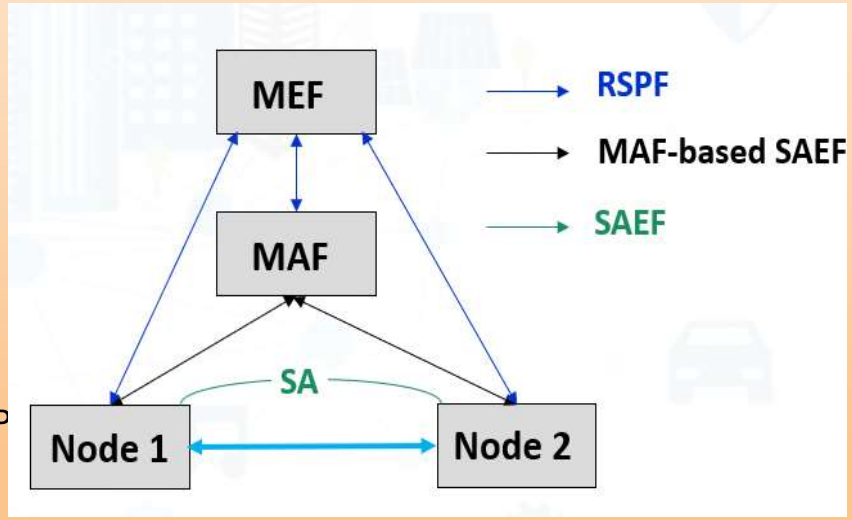
- **M2M Enrollment Function can trigger the Field Device to execute a variety of procedures, including**
  - Configuration of Field devices with registration parameters (e.g. oneM2M identifiers and contact information)
  - Provisioning of symmetric keys
  - Provisioning of certificates

  Keys and Certificates can be provisioned for securing oneM2M communication across a single communication "hop" or across multiple hops in an end-to-end fashion (see following slides).

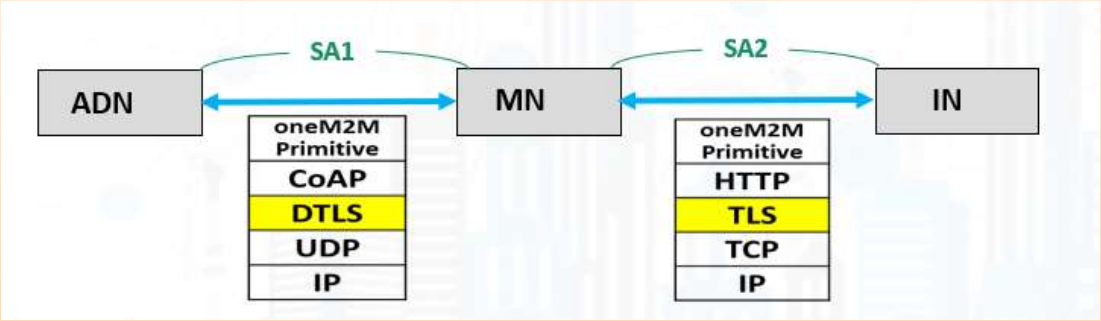
- **M2M Enrollment Function is operated by M2M Service Provider or trusted 3rd party (device manufacturer, underlying network operator, etc.)**

M2M Enrolment Function (MEF)

- M2M Enrolment Function allows 3 types of Remote Security Provisioning Frameworks (RSPF)
  - Symmetric key authenticated RSPF
  - Certificate authenticated RSPF
  - GBA-authenticated RSPF; in this case the MEF is the Bootstrapping Server Function (BSF) of 3GPP Generic Bootstrapping Architecture (GBA)
- MEF can trigger the Field Device to execute a variety of procedures, including
  - Configuration of Field devices with registration parameters and authentication profiles applicable to the operational Security Frameworks (see next slide)
  - Provisioning of symmetric key credentials
  - Provisioning of certificates (certificate (re-)enrolment using EST and SCEP specified by IETF recommendations)
- MEF is operated by M2M Service Provider or trusted 3rd party (device manufacturer, underlying network operator)



Message Security between adjacent Entities: The operational security framework



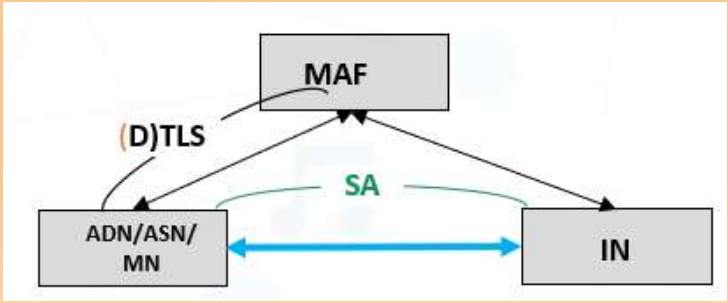
Message Security between adjacent Entities: The operational security framework

Uses (Datagram) Transport Layer Security Protocols, TLS/DTLS Version 1.2

Several Security Association Establishment Frameworks are supported:

1) Authentication and session key establishment using **symmetric keys** shared by devices
2) Authentication and session key establishment using **Certificates** provisioned to devices
3) Authentication facilitated by an **M2M Authentication Function (MAF)** hosted by M2M-SP or third-party

The MAF authenticates the end-points (PSK or certificates) and facilitates establishing a symmetric key

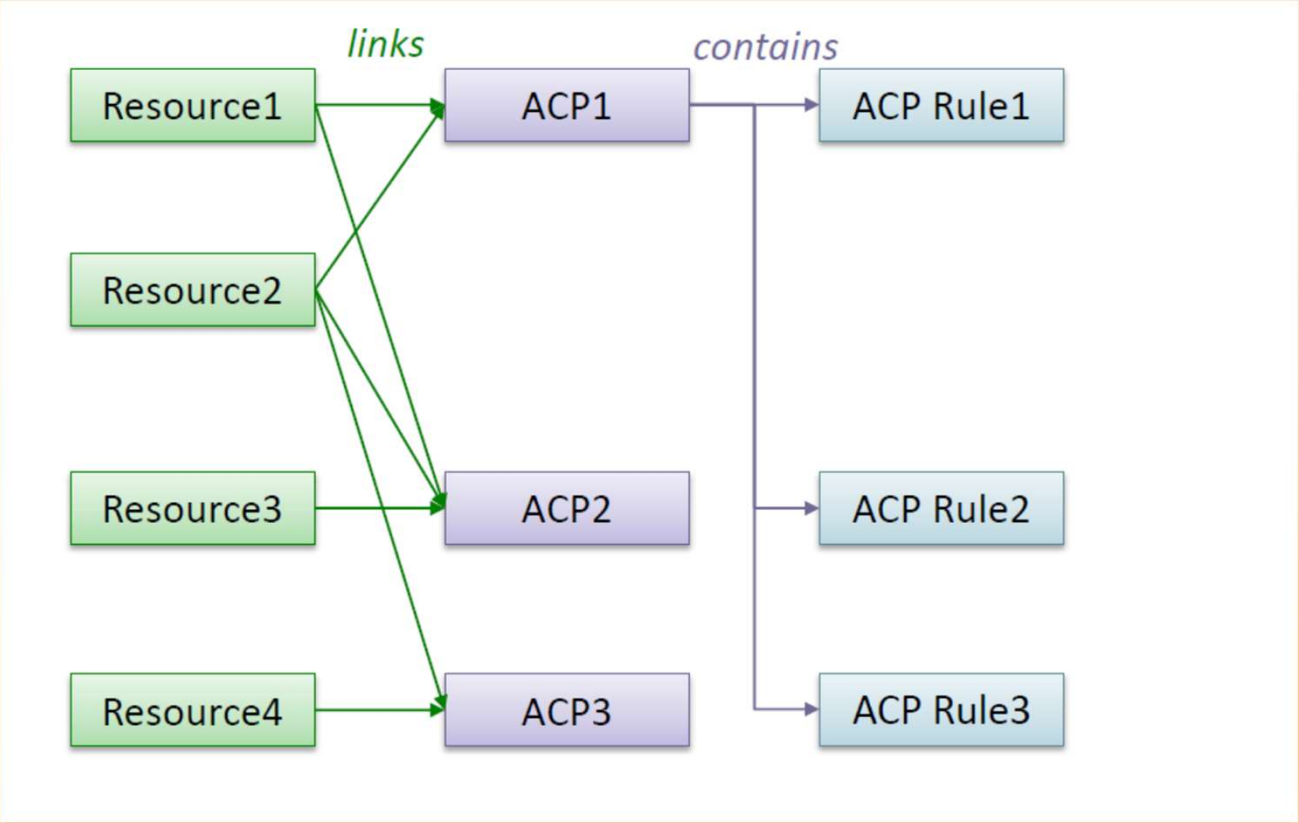


Authorization / Access Controls

- oneM2M is based on a RESTful architecture
  - API is based on requests to perform an operation on a resource
  - Operations are Create, Retrieve, Update, Delete

- oneM2M Service Layer supports **configurable access control policies** that define clear rules dictating, for each resource
  - WHO is authorized to access,
  - WHAT operations are allowed, and under
  - WHICH conditions (e.g. time, location of entity)

Authorization / Access Controls

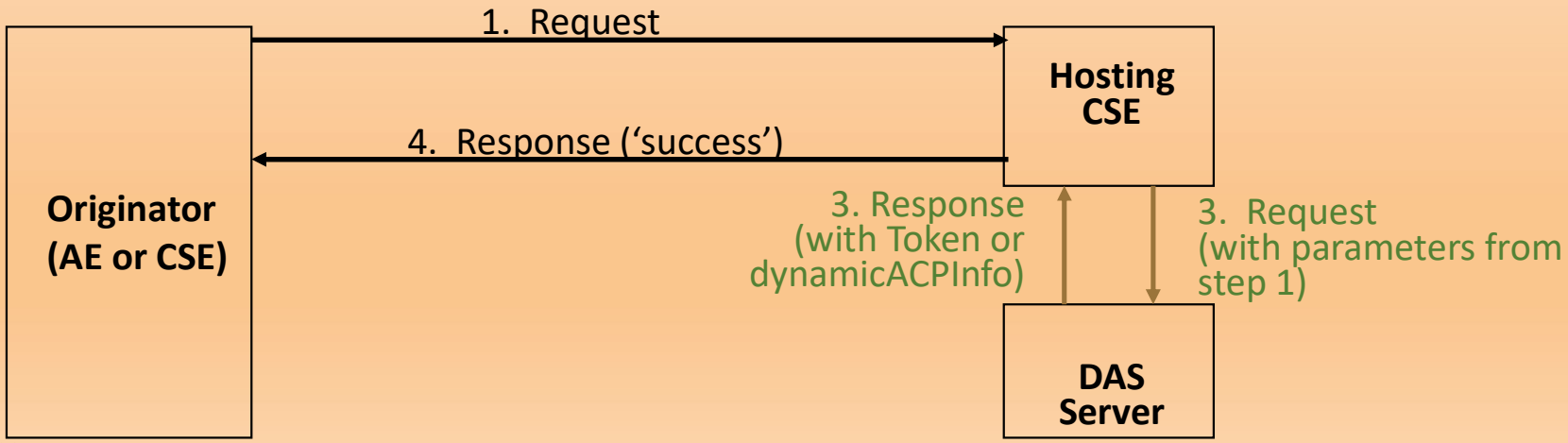


Resource access is authorized based upon satisfying at least on Access Control Policy (ACP) rule in one of the linked ACPs

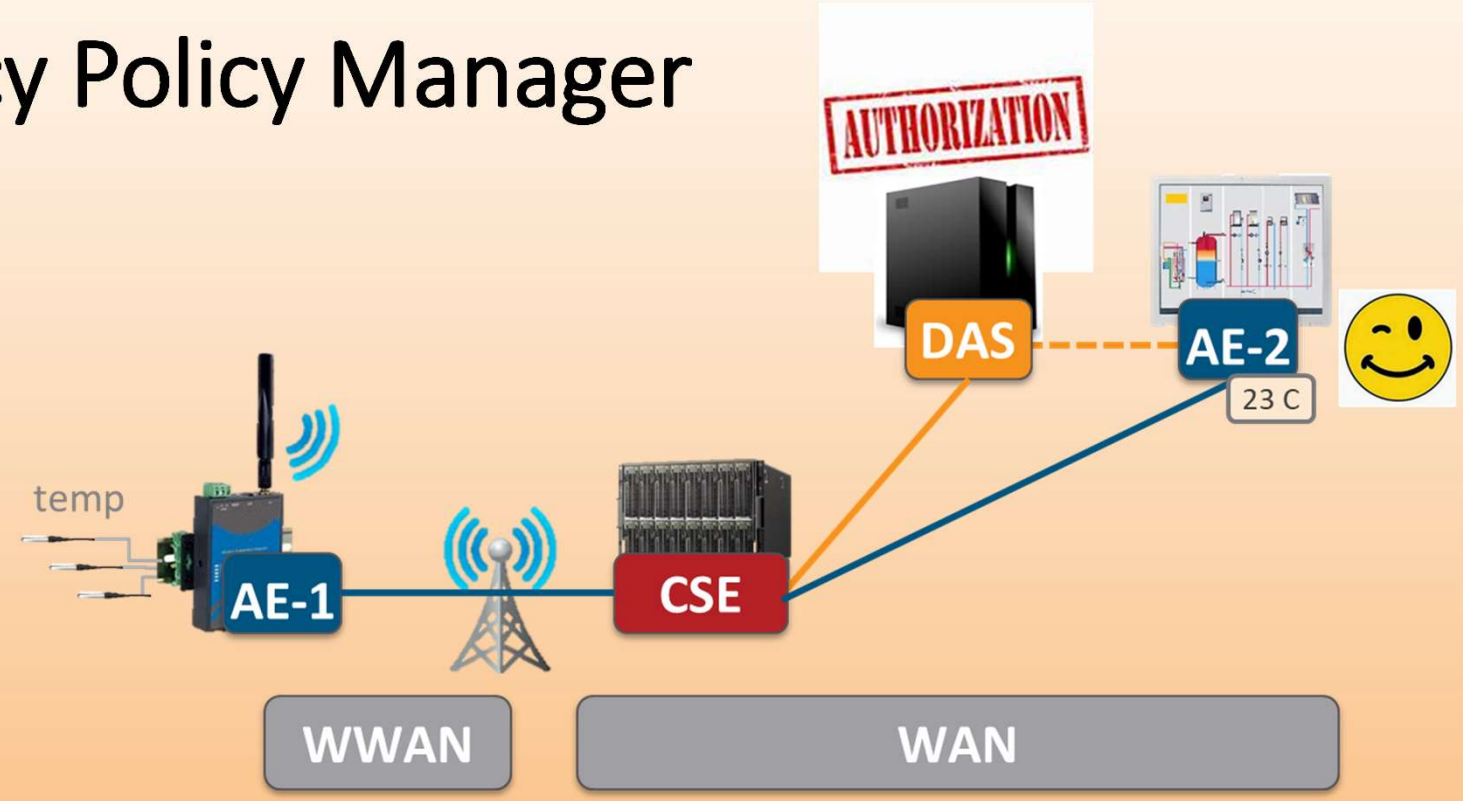
Dynamic Authorization

- **Dynamic Authorization**: Originator or Hosting CSE requesting authorization of Originator – provided by a Dynamic Authorization System (DAS) Server
  - Direct Dynamic Authorisation: Hosting CSE submits request to DAS, Originator not communicating with DAS Server
  - Indirect Dynamic Authorisation: Originator submits request to DAS Server using info provided by Hosting CSE. Similar to Open Authentication (OAuth) mechanism
  - DAS has multiple options for authorizing: Issue/update access control rules, assign Role(s) to the Originator, issue JSON Web Tokens (JWT)

Direct Dynamic Authorisation



Privacy Policy Manager



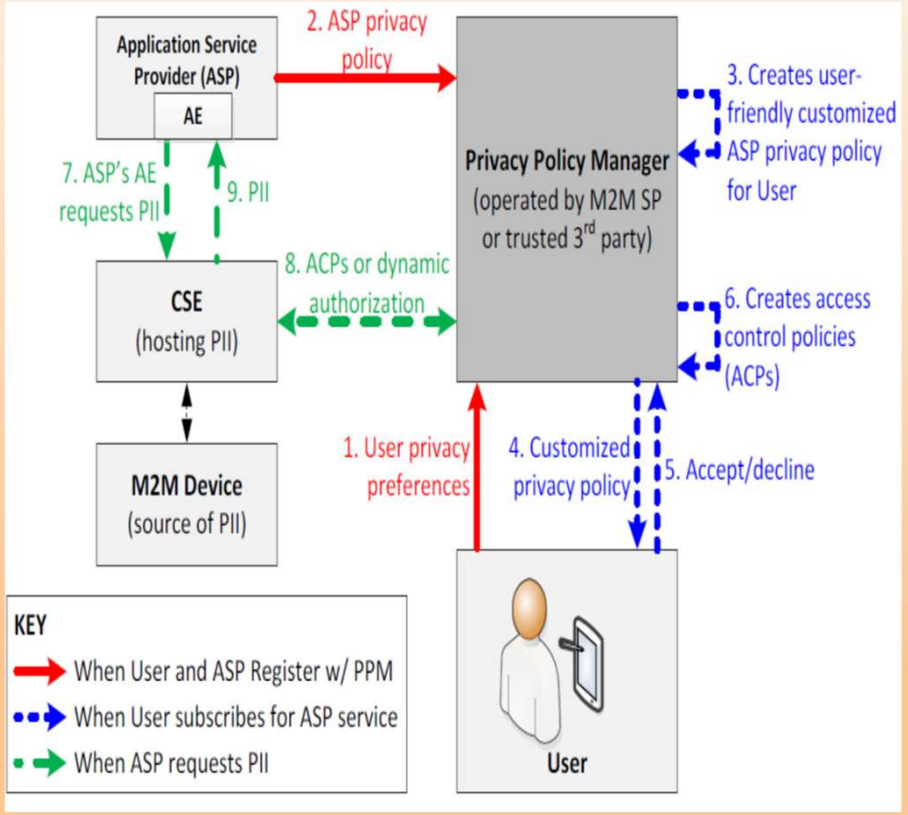
DAS: Dynamic Authorization System
AE: Application Entity
CSE: Common Services Entity

Privacy

- The PPM is a
framework
- The PPM cor
preferences
order to prot
Identifiable I
unauthorized
- Access contr
and dynamic
- PPM uses a '
language" to
User's privac
Service Provi

Privacy Policy Manager (PPM)

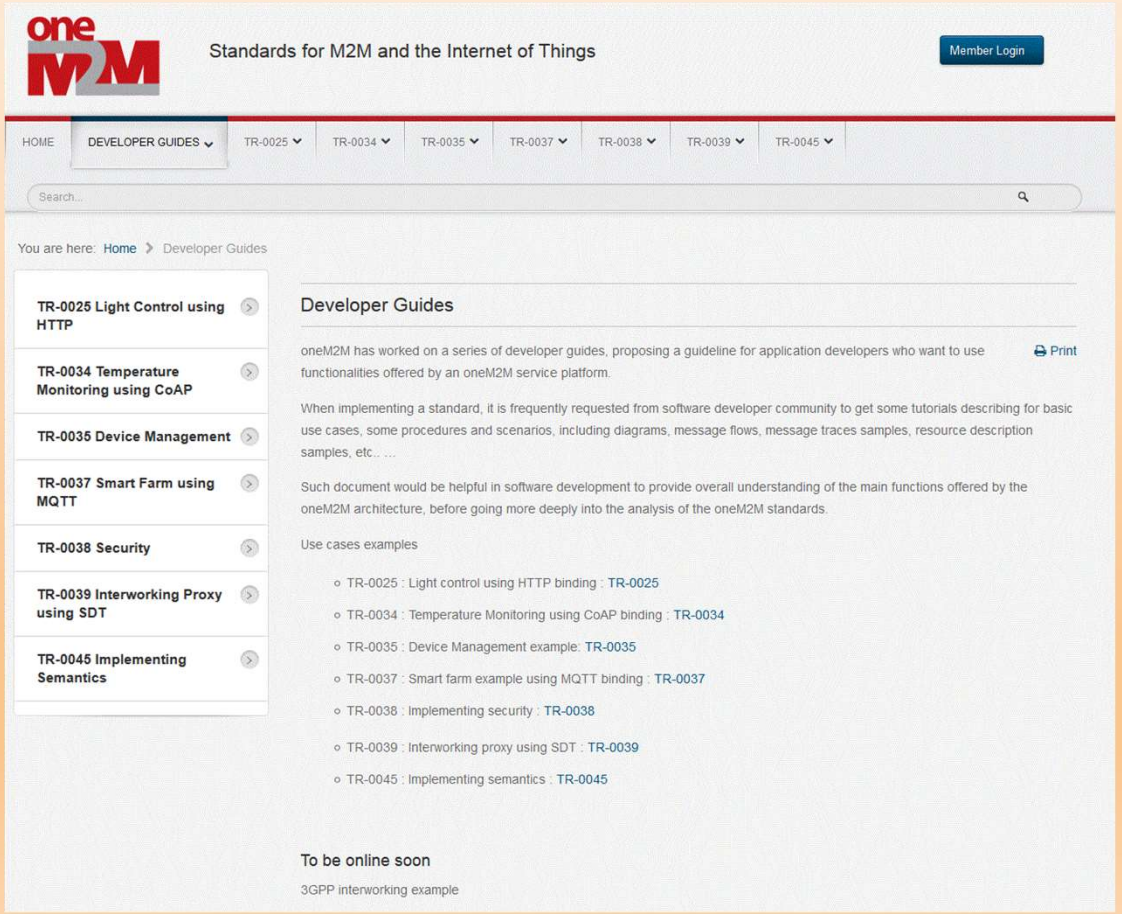
- The PPM is a personal data management framework
- The PPM converts a User's privacy preferences into access control information in order to protect the User's Personally Identifiable Information (PII) from access by unauthorized parties.
- Access control information consists of static and dynamic access control policies (ACP)
- PPM uses a "Terms and Condition's Mark-up language" to derive consensus between the User's privacy preferences and an Application Service Provider's privacy policies



Publicly Accessible Links

Developer Guides

are now accessible via the public link:
http://www.onem2m.org/developer-guides



Publicly Accessible Links:

- Web Site
  http://www.oneM2M.org
- Developer Guides
  http://www.onem2m.org/developer-guides
- Technical Questions
  http://www.onem2m.org/technical/technical-questions
- Published Specifications
  http://www.onem2m.org/technical/published-documents
- Documents developed in oneM2M
  http://www.onem2m.org/technical/latest-drafts

Webinars
http://www.onem2m.org/technical/webinars

YouTube Channel
https://www.youtube.com/c/onem2morg

Events
http://www.onem2m.org/news-events/events

Thank You!

For any questions, please email rana.kamill@bt.com

From Computers to "Things"

Internet of Computers

- Attended by **human** « owners »
- Comfortable, controlled **environment**
- Relatively fixed **location**
- Low latency broadband **connection**
- **Few chipsets and OSs** to secure
- **Few Apps largely deployed**
- Rather **uniform lifetime**
- Relatively **powerful resources** (computing, memory, energy supply)
- Billions of **targets** online
- Internet as **entry point**
- Frequent software **security patches**
- Ever decreasing **cost of attacks**
- « ***Virtual world*** » **impact** (information)

Internet of Things

- Largely **unattended** by owners
- Harsh conditions, or physical **exposure**
- Potentially highly **mobile**
- **Sporadic/constrained** throughput/latency
- **Diversity** of embedded hard and soft
- **Multitude of small deployments**
- **Lifetime from months to decades**
- **Constrained** power, memory, processing

- 100s of billions of targets!
- More, weaker entry points
- Weaker, possibly unmaintained software
- Available and accessible
- ***Real world*** **impact** (physical safety)

Security in an IoT architecture: Tough challenges

- Very large attack surface
- Limited device resources
- Complex ecosystem: rich and connected ecosystem
- Fragmentation of standards and regulations
- Widespread deployment
- Security integration: heterogeneous secured systems
- Safety aspects: interaction with real word
- Low cost constraint
- Security update
- Insecure programming: time to market
- Unclear liability

Source: Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, ENISA, November 2017

IoT Architectures evolution

« IoT 1.0 »

Upstream Sensor data acquisition to Big Data Analytics in the Cloud

- Primarily concerned with exploiting huge amount of information
- Centralized, many clients to one server,
- Predictable, asynchronous connections addressed by traditional cybersecurity
- Privacy as a main security driver

« IoT 2.0 »

Closed loop autonomous system with downstream actuators control

- Rather concerned with processing time for feedback loop
- Distributed, many-to-many, multi-roles, dynamic, real-time connections
- critical infrastructures require physical protection in addition to cybersecurity
- Human safety as a strong security driver

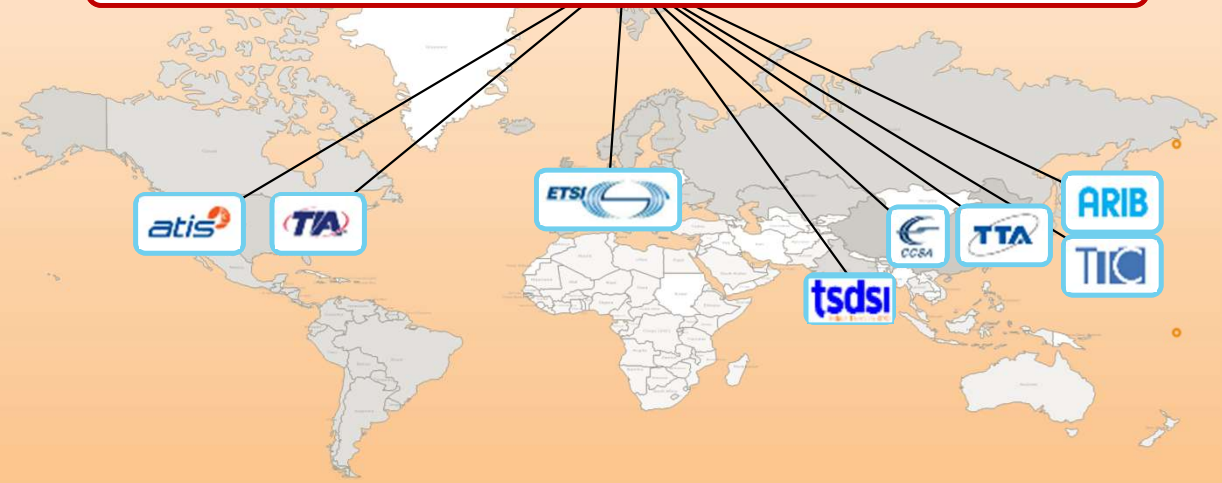
About oneM2M

The Global Partnership Initiative
Standardizing an Open Horizontal M2M Service Layer Platform

Motivation for oneM2M: Consolidation

Global partnership initiative:
Consolidate standardization of M2M/IoT functions

~200 member organizations in oneM2M

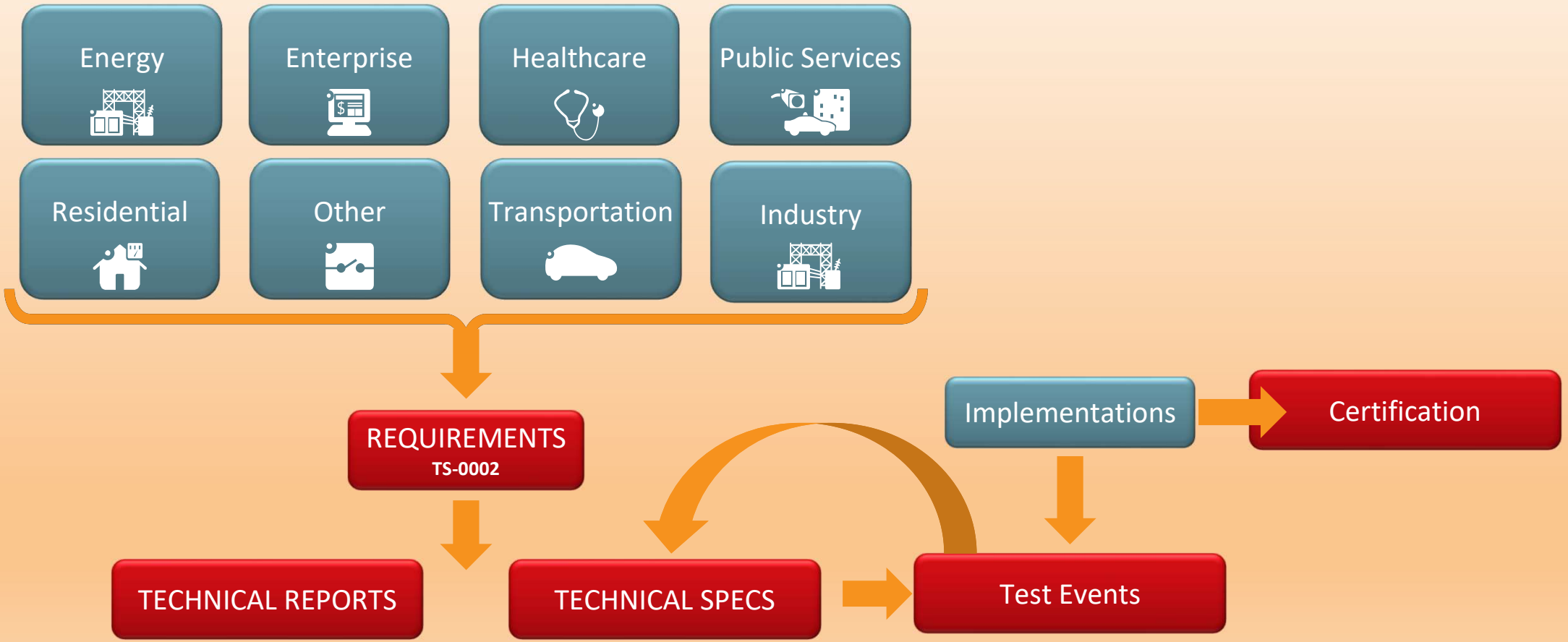


broadband forum · oma · CEN CENELEC · GLOBALPLATFORM

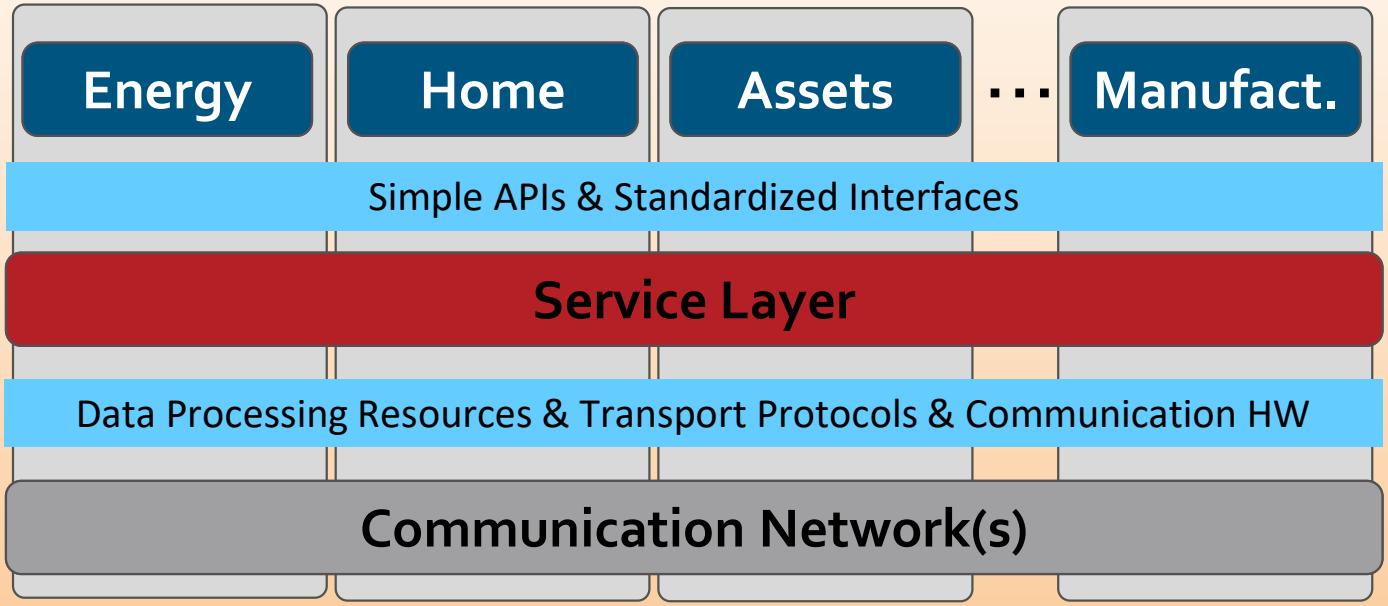
one M2M

- Partner Type 1: **ARIB, ATIS, CCSA, ETSI, TIA, TTA, TTC & TSDSI**
- **All major Telecom SDOs around globe**
  - Members (e.g. companies) participate in oneM2M via admitting Partner Type 1
  - IPR policy of admitting Partner Type 1 organization is binding for members
  - Partner Type 1 organizations are committed to transpose specifications into standards
- Partner Type 2: BBF, CEN/CENELEC, New Generation M2M Consortium, OMA, Global Platform
  - Fora/Associations/Consortia participate & contribute in oneM2M with compatible IPR regime
- Milestones
  - Created in 2012, avoiding standards fragmentation
  - Published Rel-1 Q1/15, Rel-2 Q3/16, Rel-2a Q1/18, Rel-3 Q3/18
  - 6 interop test events so far, several developer events and hackathons
  - Open source implementations (8), commercial take up

Work Process



oneM2M: Standard for M2M / IoT

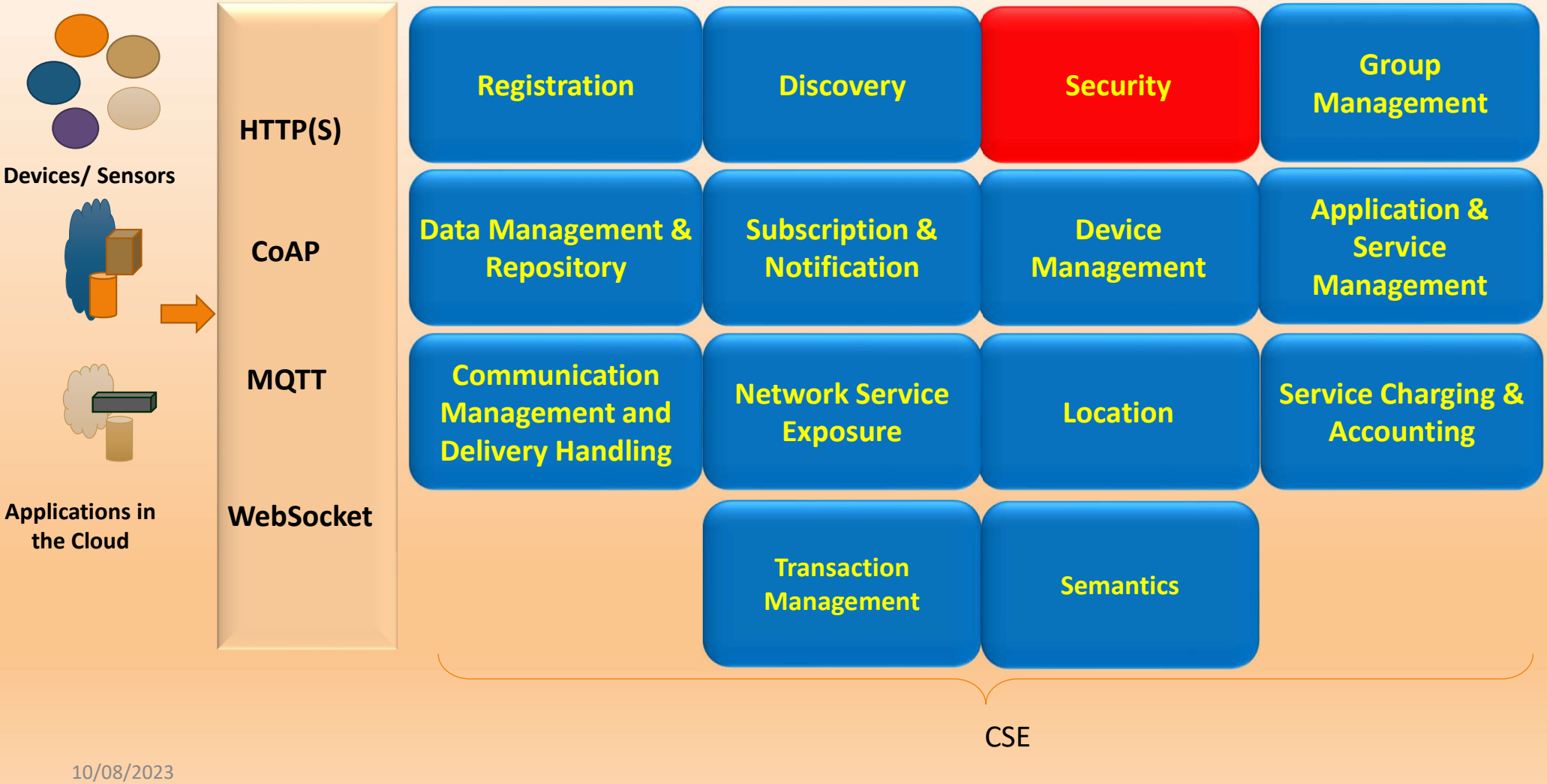


Horizontal layer of functions commonly needed across different market segments / not segment-specific

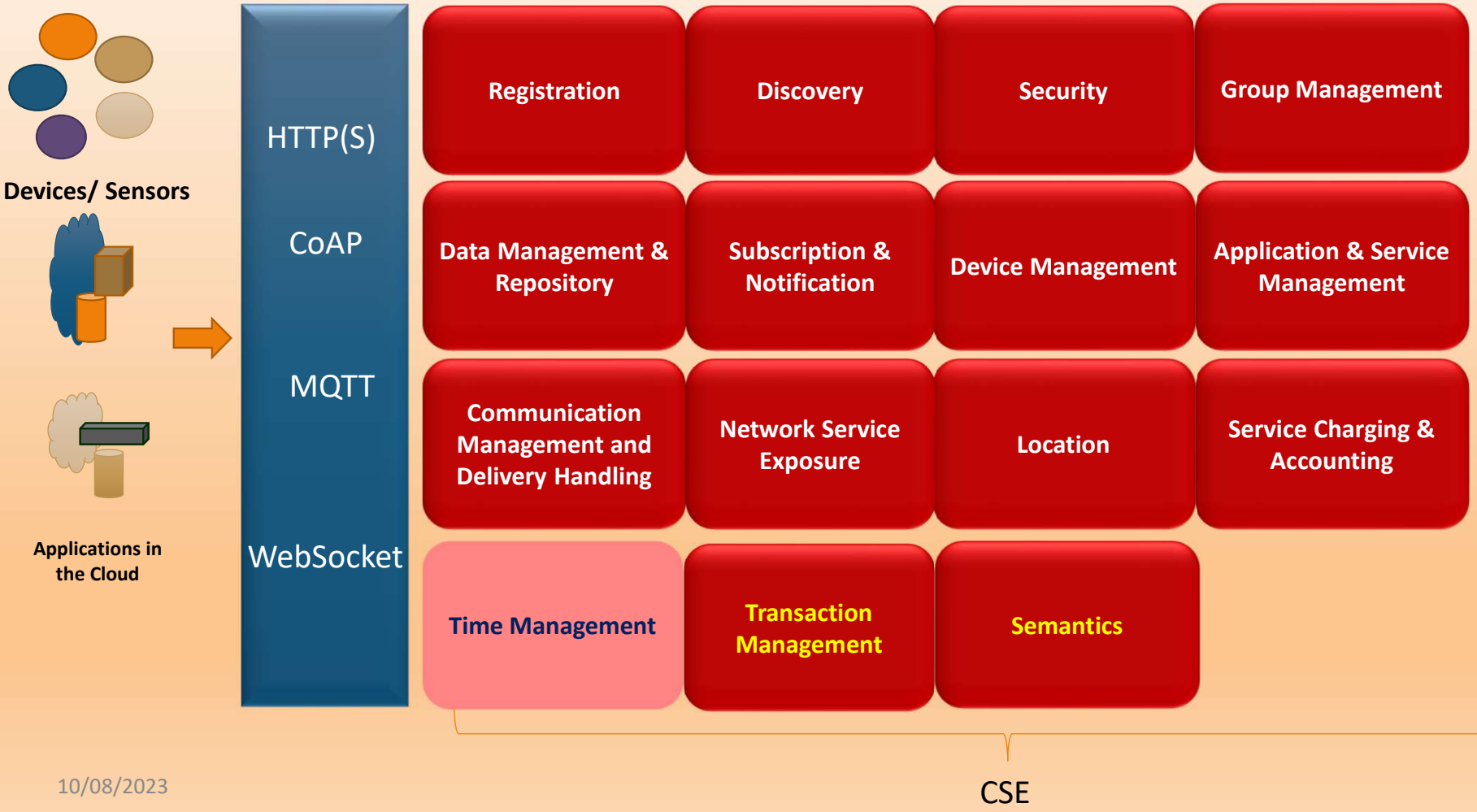
Similar to generic versus use case-specific computer/OS in early times of computers

- Standard for a middleware platform
- Sits between applications and processing/communication HW
- On sensors, actors, gateways, cloud
- Authentication/authorization/encryption
- Connects producers/consumers securely
- Hides complexity of NW usage from apps
- Controls when communication happens
- Increases efficiency of data transport
- Stores and shares data
- Supports access control
- Notifies about events
- Talks to groups of things
- Device & life cycle manages, large scale

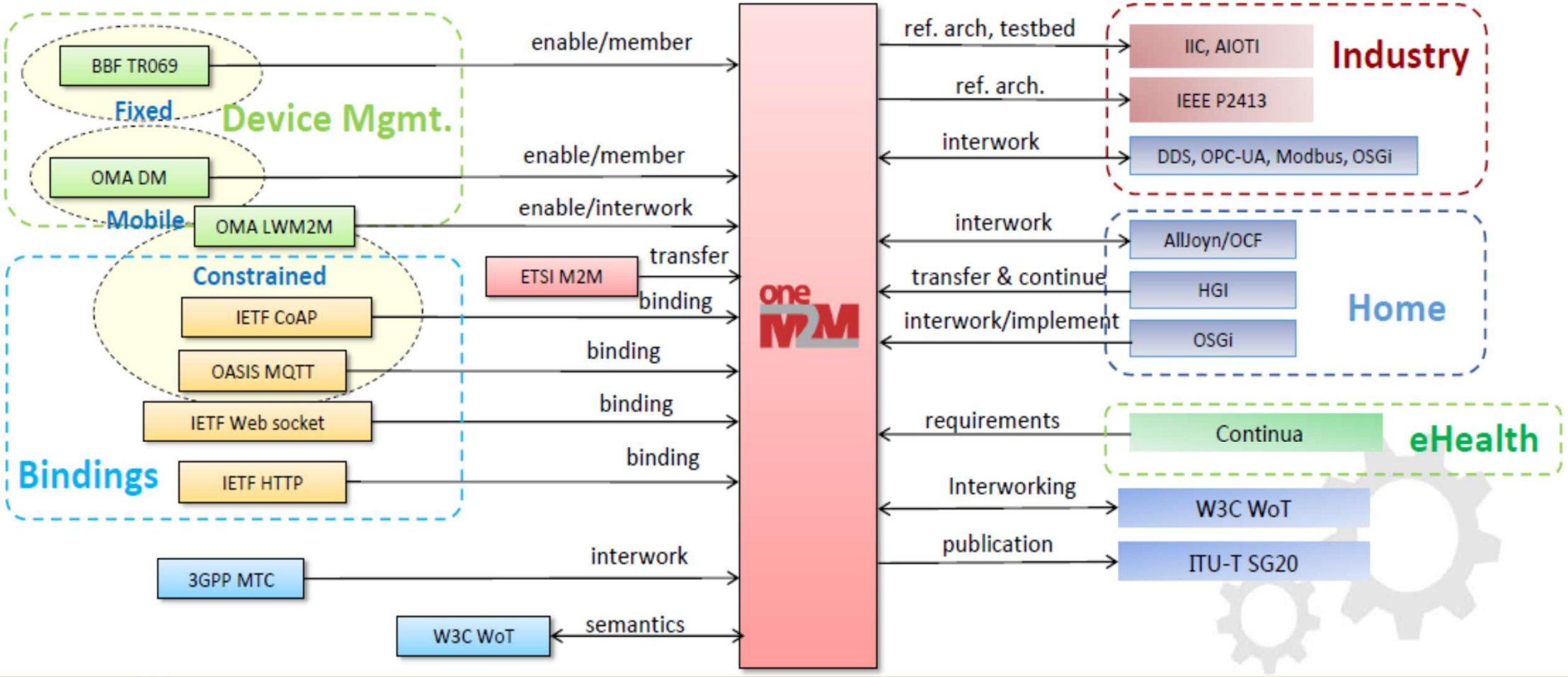
The Common Service Functions in oneM2M Architecture



The Common Service Functions in oneM2M Architecture

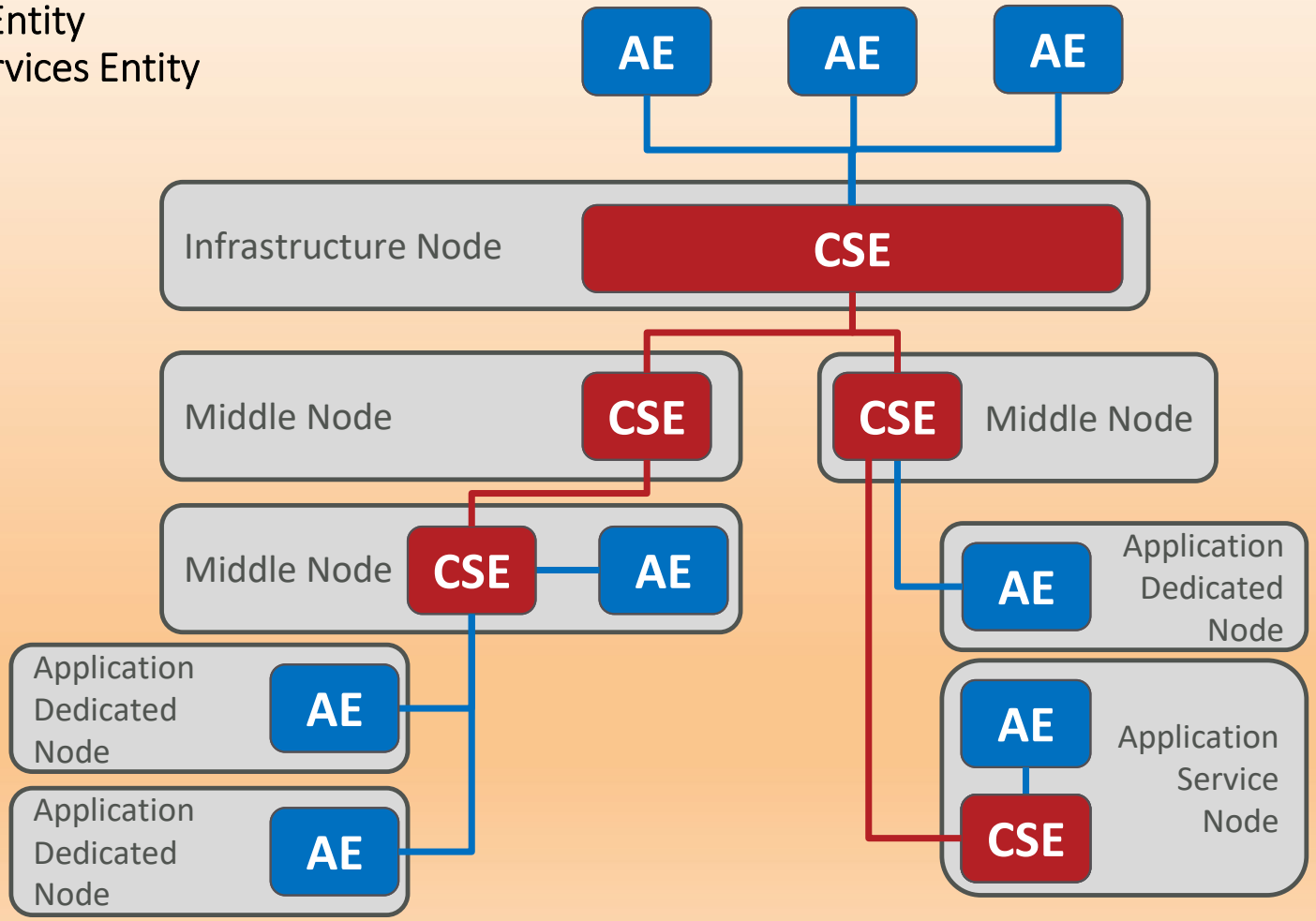


Industry collaboration around oneM2M



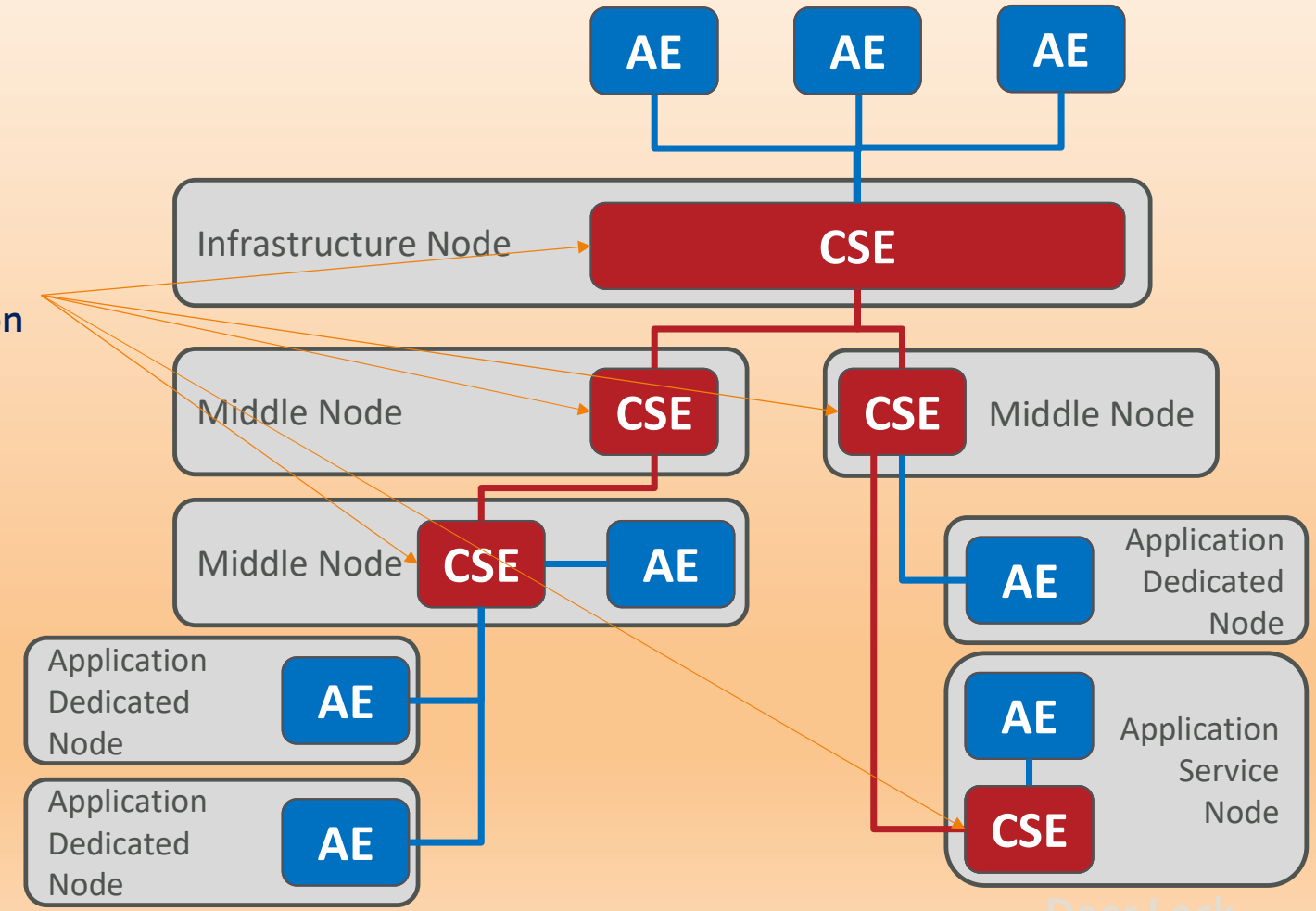
Topology

AE: Application Entity
CSE: Common Services Entity



RESTful Style & Access Control

Resources
= State Information



oneM2M Feature Summary by Release

Rel-1 Features

- Registration
- Discovery
- Security
- Group Mgmt.
- Data Mgmt. & Repository
- Subscription & Notification
- Device Management
- Communication Mgmt.
- Service Charging
- Network Service Exposure
- App & Service Mgmt.
- HTTP/CoAP/MQTT Bindings

Rel-2 Features

- Time Series Data
- Flexible resources that can be customized by app developers
- Semantics Description & Discovery
- Security Enhancements
  - Dynamic Authorization
  - Content Security
  - E2E Security
- WebSocket Binding
- Ontology for Home Area Information Model
- oneM2M App-ID Registry
- oneM2M Interworking
  - LWM2M
  - AllJoyn
  - 3GPP Triggering

Rel-3 Features

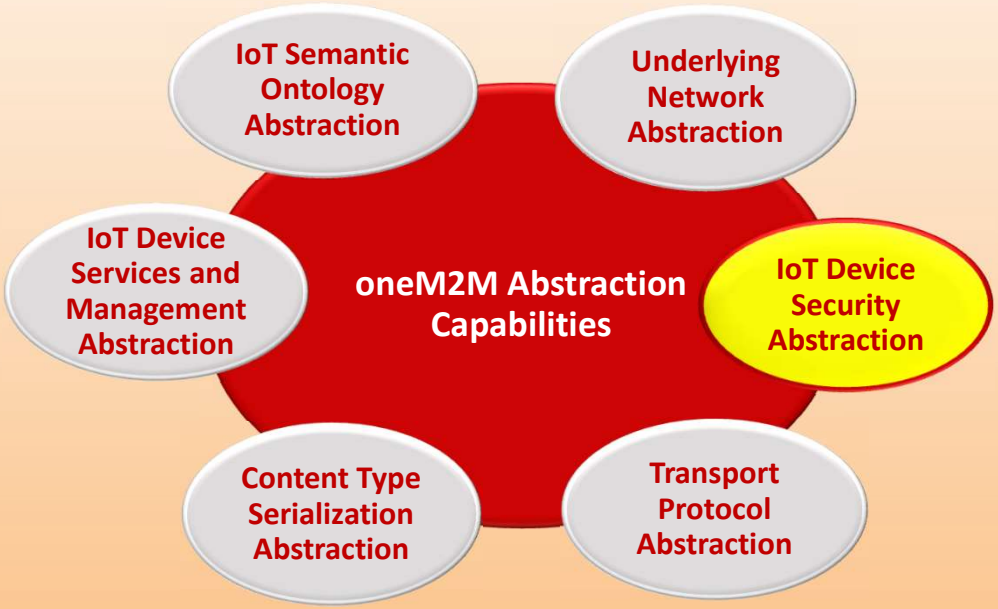
- Semantic Querying/Mashups
- 3GPP SCEF Interworking
  - Non-IP Data Delivery,
  - UE Reachability Monitoring
  - Device Triggering
  - Etc.
- Transaction Management
- Service Layer Routing
- Common oneM2M Interworking Framework
  - OCF, OPC UA, OSGi, Modbus
- oneM2M Conformance Tests and Profiles
- Security Enhancements
  - Distributed Authorization, etc.
- Ontology-based Interworking

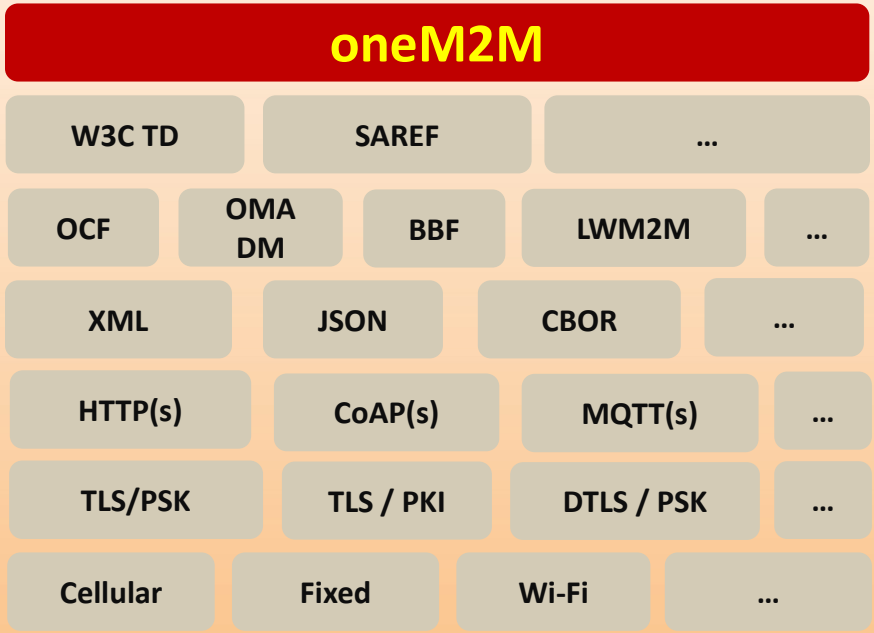
Rel-4 Features (planned)

- Fog/Edge Computing
  - Service Provisioning
  - Service Pooling, etc.
- 3GPP Interworking
  - Session QoS
  - V2X
  - NIDD Enhancements
  - Charging
- Vehicular Centric Features
  - Mobility, low latency, …
- Semantic Reasoning & Ontology Mapping
- Service/User Subscription
- Security Enhancements
  - User/Data Privacy, etc.
- W3C WoT Interworking
- SDT4.0 and the information models for multiple domains
- Streamlining oneM2M protocol
- oneM2M Conformance Tests

oneM2M's Value Proposition to Developers

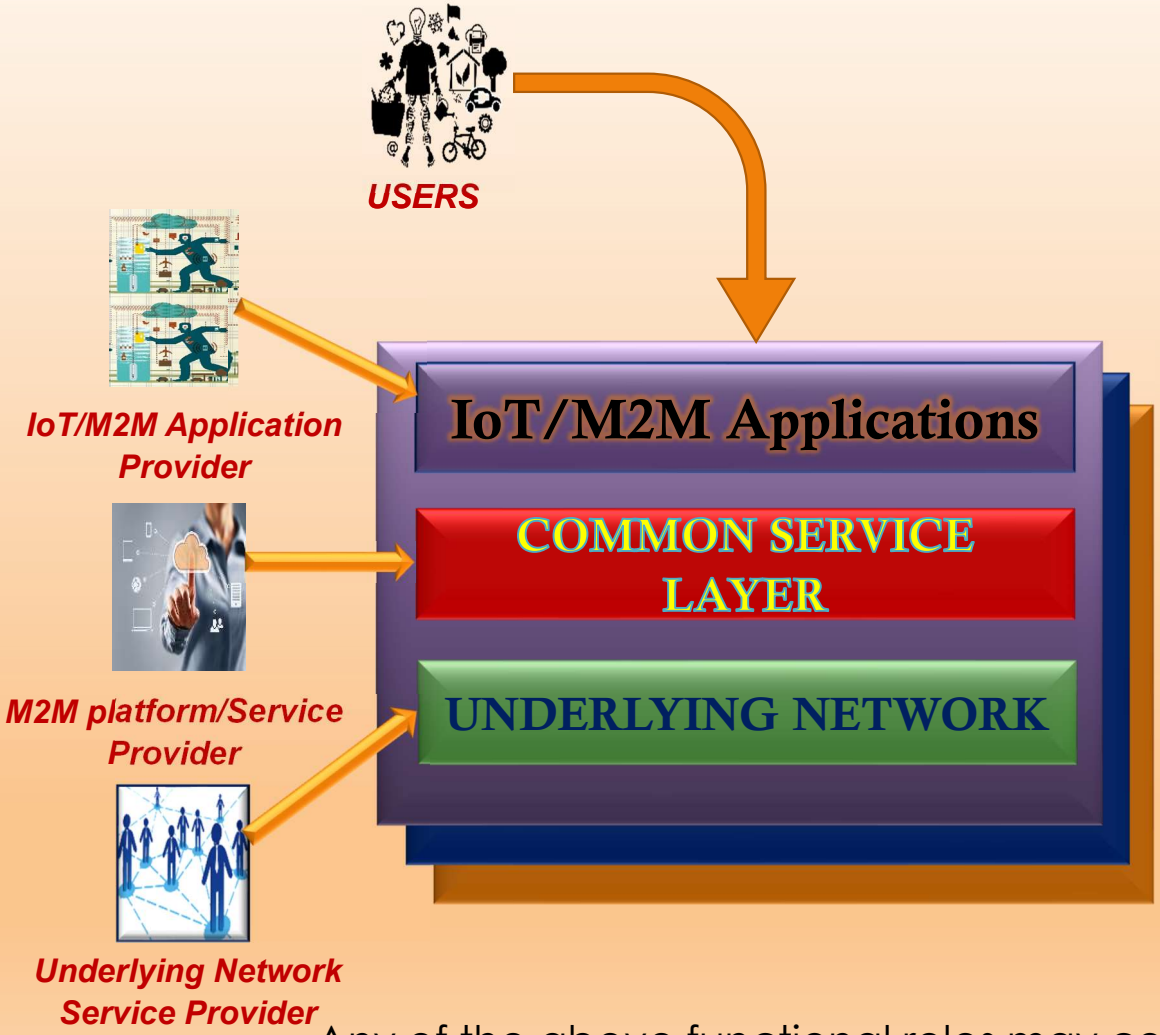
- → ***Abstraction, Abstraction, Abstraction!***





→ Via its capabilities to abstract, oneM2M hides from the App Developer the complexities involved to interact with the diversity of IoT devices

Functional Roles in the M2M Ecosystem



Functional Role Description

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

Any of the above functional roles may coincide with any of the other roles.
These functional roles do not imply business roles or architectural assumptions.

Security in oneM2M

Release 2- Release 3

Main security functions supported

- Identification and Authentication
  - Identification: checking if the identity of the request originator provided for authentication is valid
  - Authentication: validating if the identity supplied in the identification step is associated with a trustworthy credential
- Security Association Establishment
  - Establishment of a security context between communicating entities to provide confidentiality (encryption) and integrity
  - Range of authentication options supported
- Authorization (“Access Control”)
  - Authorizing services and data access to authenticated entities
- Remote Provisioning

Additional security functions

- Identity protection
  - Capability to use pseudonyms to protect anonymity of transactions
- Sensitive data handling
  - Capability to protect sensitive data (e.g. local credentials) and functions (e.g. data encryption/decryption) in a Secure Environment (e.g. Smart Card or Virtual Smart Cart)
- Security administration (related to device management)
  - Creates and administers dedicated Secure Environments and postprovisioning of master credentials

oneM2M Secure Environment and security levels

- ‘Secure Environment’ concept abstracts the security implementation
  - Expose common services to applications, depending on implementation
  - Provide common interface for remote security administration, if needed
- oneM2M supported implementations distinguish 4 security levels
  - No additional security
    - devices otherwise protected from attackers, i.e. on trusted networks
  - Software only security (obfuscation, White box crypto etc.)
    - Always vulnerable to sufficiently motivated attacker
    - Acceptable when compromise is not critical
  - ‘Trusted Execution Environment (TEE)’ relying on main CPU hardware features
    - Good barrier against software based attacks
    - Sufficient for remotely accessible, but not physically exposed devices
  - Tamper resistant hardware Secure Element ((e)SE, (e)UICC)
    - Required to protect secrets within devices physically exposed to attackers (SPA / DPA etc.)
      e.g. to protect unattended devices against cloning

Security in oneM2M Release 2- Release 3

Expose security services to IoT applications

Enrolment services (Remote Security Provisioning / M2M Enrolment Function)

Credentials Provisioning / Device onboarding / Security Configuration of the M2M System

Secure communication services (Security Association Establishment / M2M Authentication Function)

Methods for Securing Information (PSK / PKI / Trusted Party)

Point-to-point and end-to-end solutions (TLS / DTLS)

Access Control & Authorization services

Requester Authentication

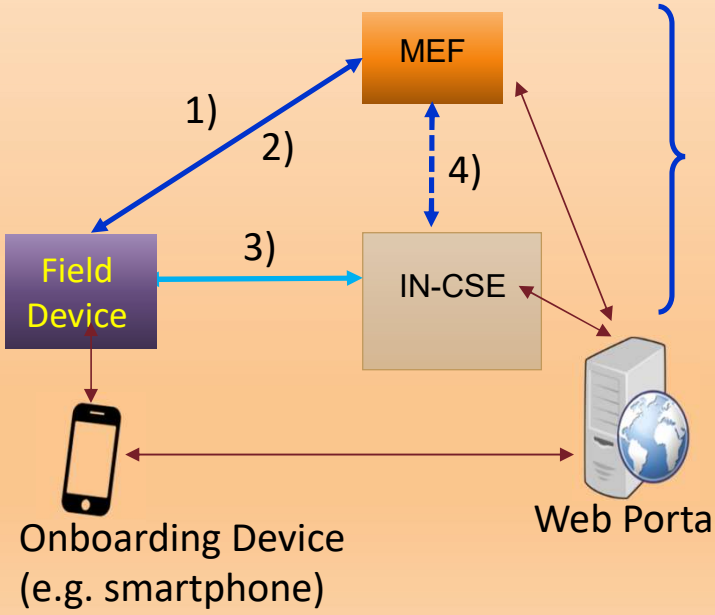
Information access Authorization

Static (ACL based) and Dynamic (token based) solutions

Privacy Policy Management

Onboarding oneM2M field devices

- Onboarding is the procedure of bringing M2M Field Devices into operation in an M2M network
- Procedures must cope with large variety of field devices types and Service Provider‘s business models
- oneM2M has specified an “M2M Enrolment Function (MEF)” which enables stakeholders to setup their preferred onboarding and enrolment mechanisms in an interoperable way

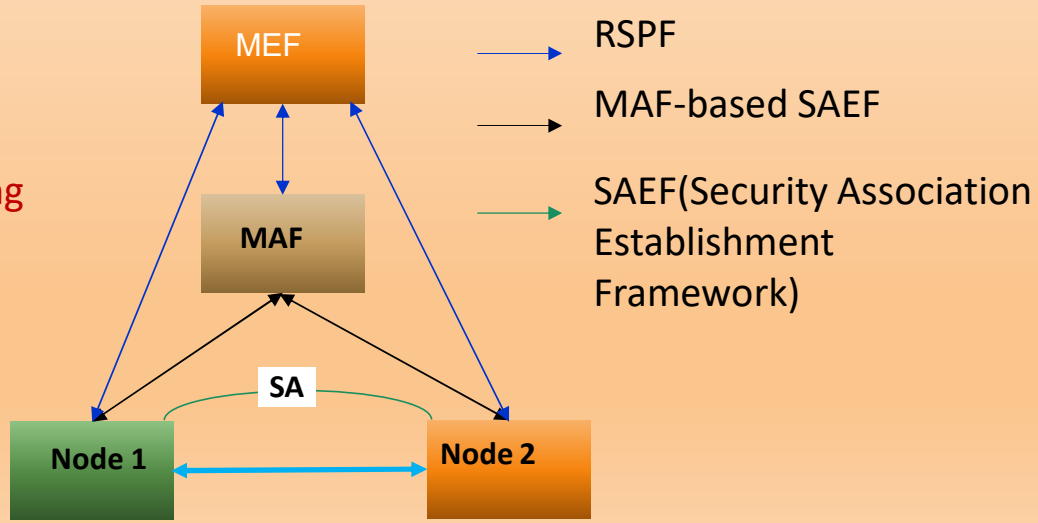


1) Field Device, provisioned with initial credentials, contacts MEF.
2) MEF configures Field Device with parameters and credentials of a Service Provider (IN-CSE)
3) Field device sends registration request to IN-CSE
4) IN-CSE authenticates the Field Device

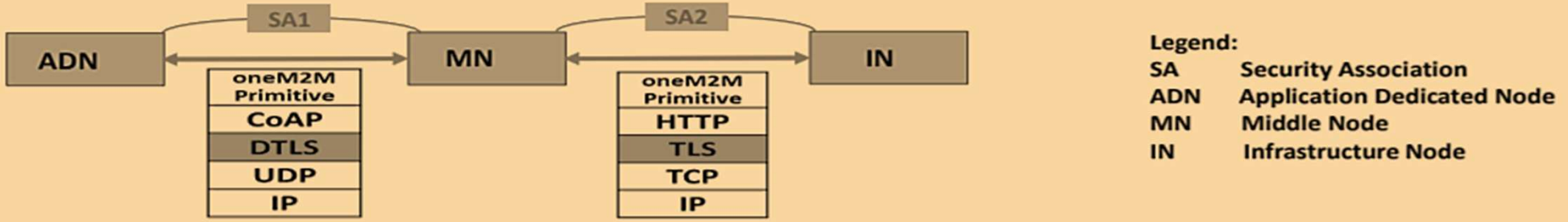
optional,
not in scope of
oneM2M specifications

Enrolment for M2M Services: Remote Security Provisioning Frameworks (RSPF)

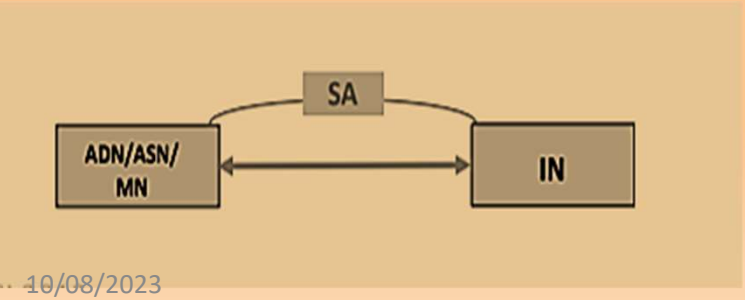
- M2M Enrolment Function (MEF) allows 3 types of Remote Security Provisioning Frameworks (RSPF)
  - Symmetric key authenticated RSPF
  - Certificate authenticated RSPF
  - GBA-authenticated RSPF; in this case the MEF is the Bootstrapping Server Function (BSF) of 3GPP Generic Bootstrapping Architecture (GBA)
- MEF can trigger the Field Device to execute a variety of procedures, including
  - Configuration of Field devices with registration parameters and authentication profiles applicable to the operational Security Frameworks (see next slide)
  - Provisioning of symmetric key credentials
  - Provisioning of certificates (certificate (re-)enrolment using ESTand SCEP specified by IETF recommendations)
- MEF is operated by M2M Service Provider or trusted 3rd party (device manufacturer, underlying network operator)

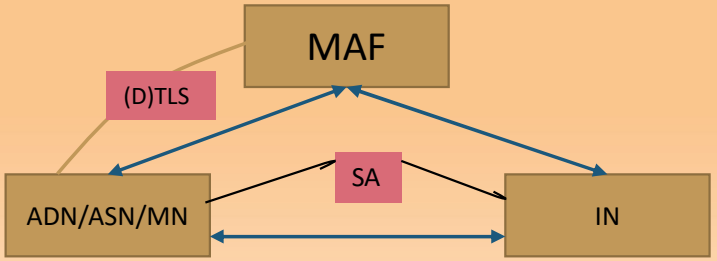


Message Security between adjacent Entities: The operational security framework



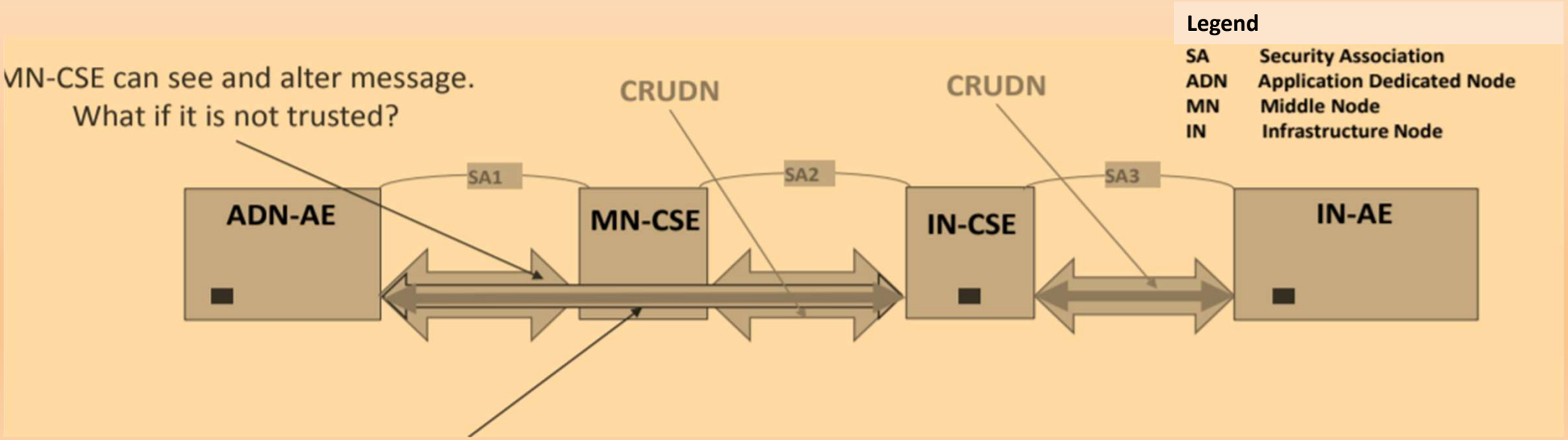
- Uses (Datagram) Transport Layer Security Protocols, TLS/DTLS Version 1.2
- Several Security Association Establishment Frameworks are supported:
  1) Authentication and session key establishment using symmetric keys shared by devices
  2) Authentication and session key establishment using Certificates provisioned to devices
  3) Authentication facilitated by an M2M Authentication Function (MAF) hosted by M2M-SP or third-party
  - The MAF authenticates the end-points (PSK or certificates) and facilitates establishing a symmetric





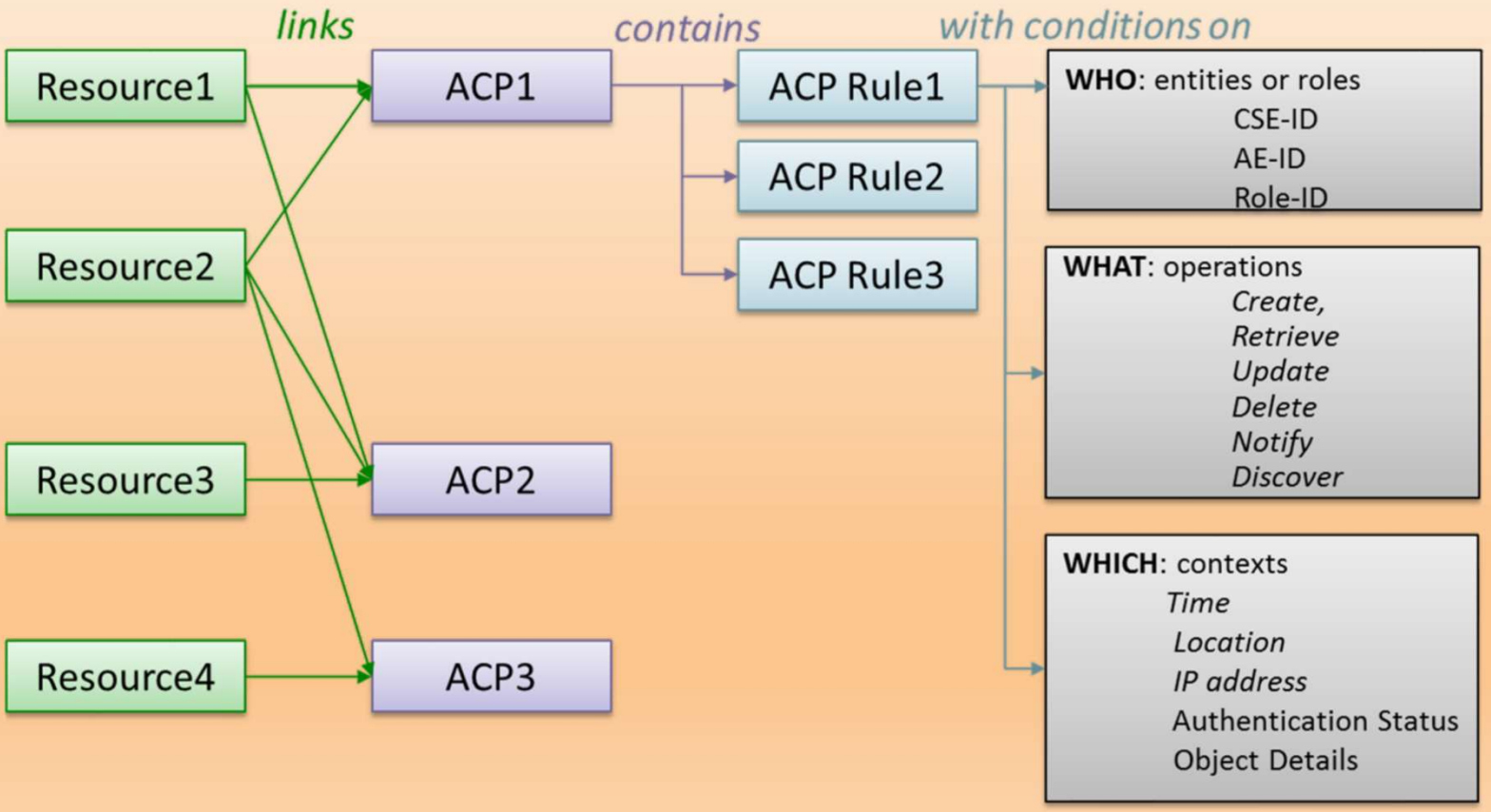
Operational Security Frameworks

- Tie together credential management, configuration parameters, establishing security session (by TLS/DTLS handshake) and protecting the messages or data
  - Security Association Establishment Framework (SAEF): Adjacent entities
  - End-to-End Security of Primitive (ESPrim): Originator ↔ Hosting CSE
  - End-to-End Security of Data (ESData): Data producer to data consumer



Authorization using Access Control Lists

- Access control rules define *who* can do *what* under *which* circumstances



Thanks