Security Conference

Security in oneM2M

Rana Kamill

IoT Ecosystems Architecture Solution Manager, BT

Senior Representative, oneM2M.

06/12/2023

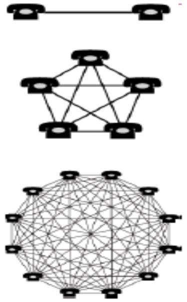
An integrated solution is needed

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

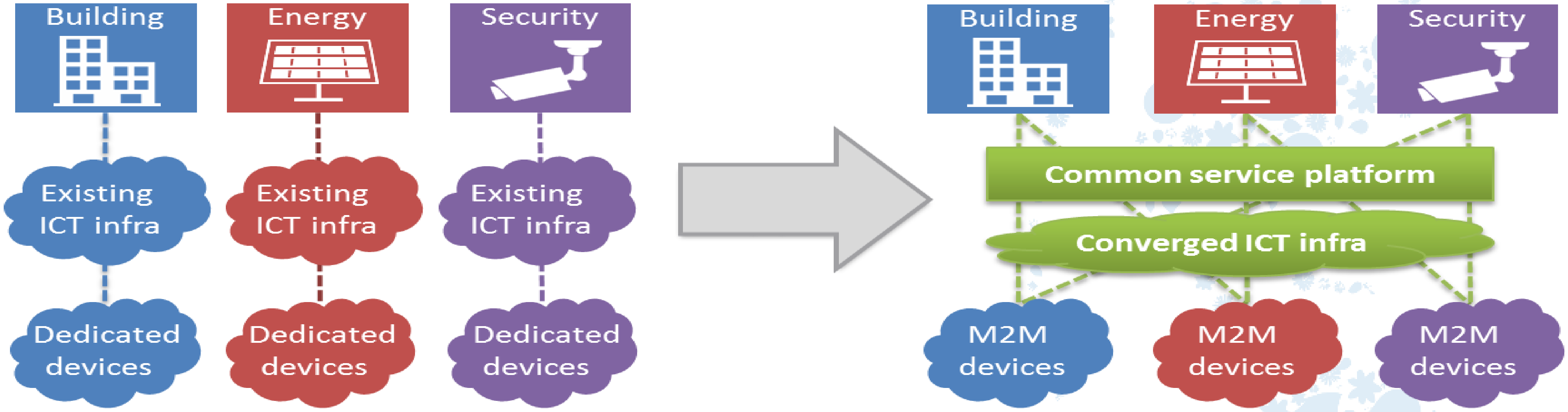
Point-to-point Integrations don't scale



Creating new integrations is unpredictable

Monocultures lock you in

Past choices restrict present action and future vision



Building

Energy

Security

Existing ICT infra

Existing ICT infra

Existing ICT infra

Dedicated devices

Dedicated devices

Dedicated devices

Building

Energy

Security

Common service platform

Converged ICT infra

M2M devices

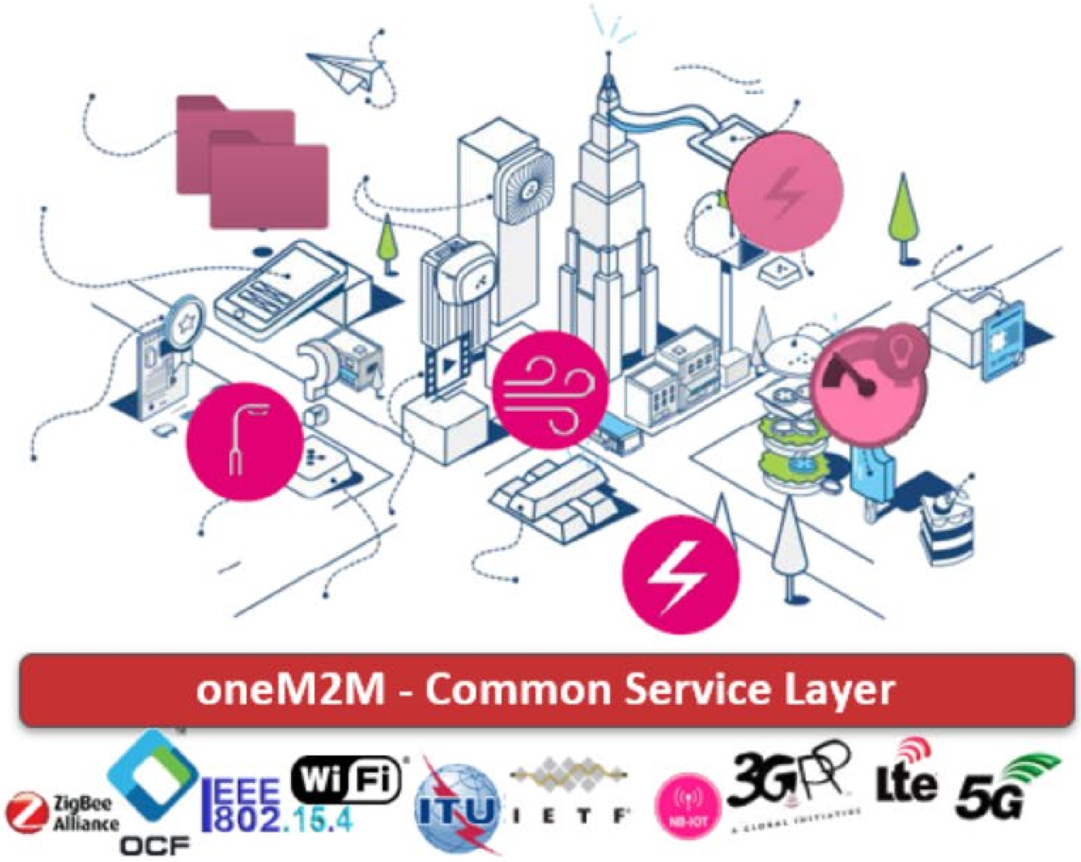
M2M devices

M2M devices

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.**

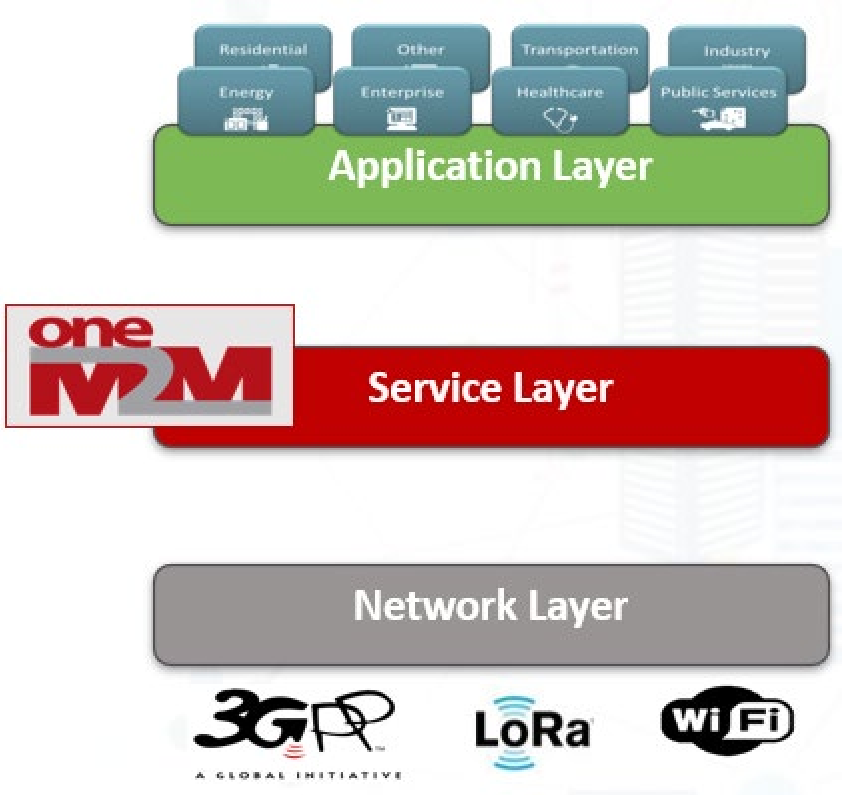


oneM2M - Common Service Layer

oneM2M

- Open global de-jure Standard
- Specifies a common set of horizontal IoT services
- Interworks with existing IoT technologies
- Value proposition
  - Simplifies the life for IoT stakeholders
  - Minimize development, deployment and maintenance costs
- Interoperability testing and certification program
- Mature and commercially deployed technology
- Vendor independent => Essential building block for an IoT ecosystem

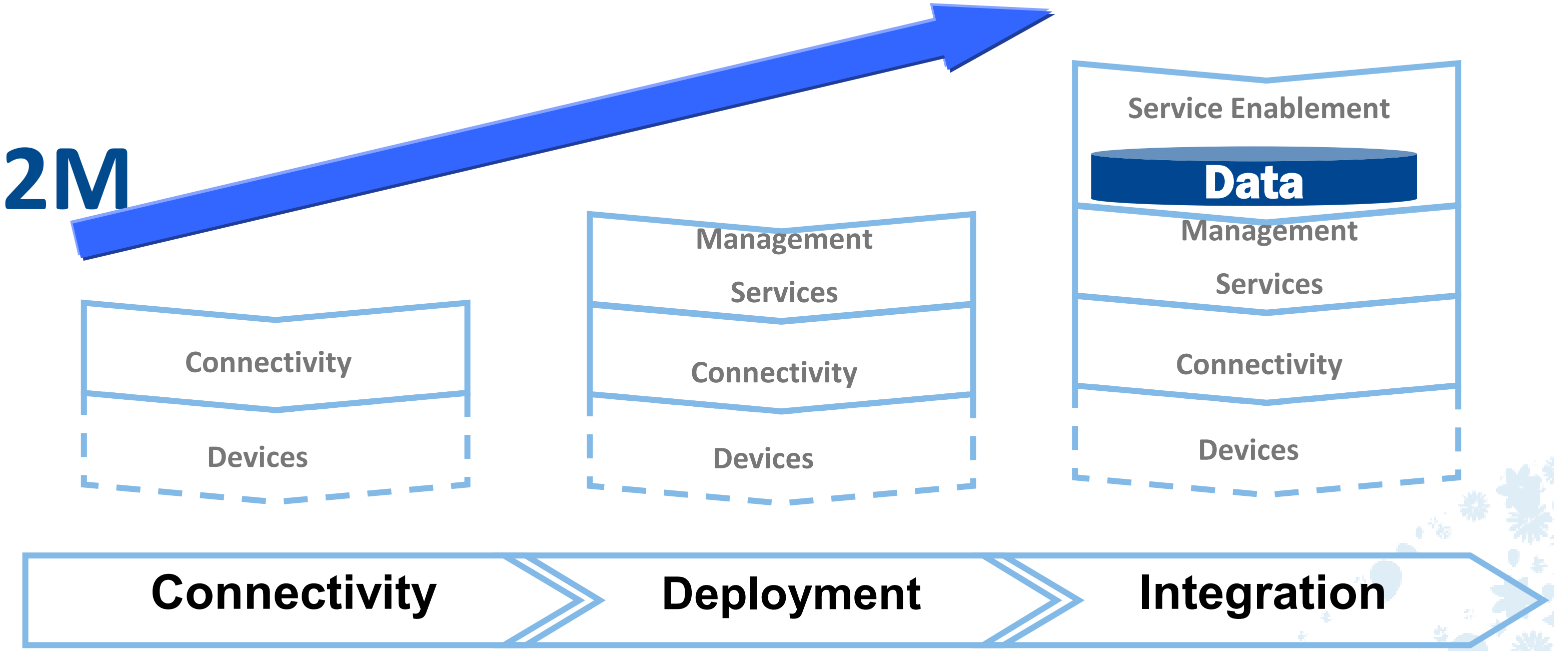
oneM2M



- 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**

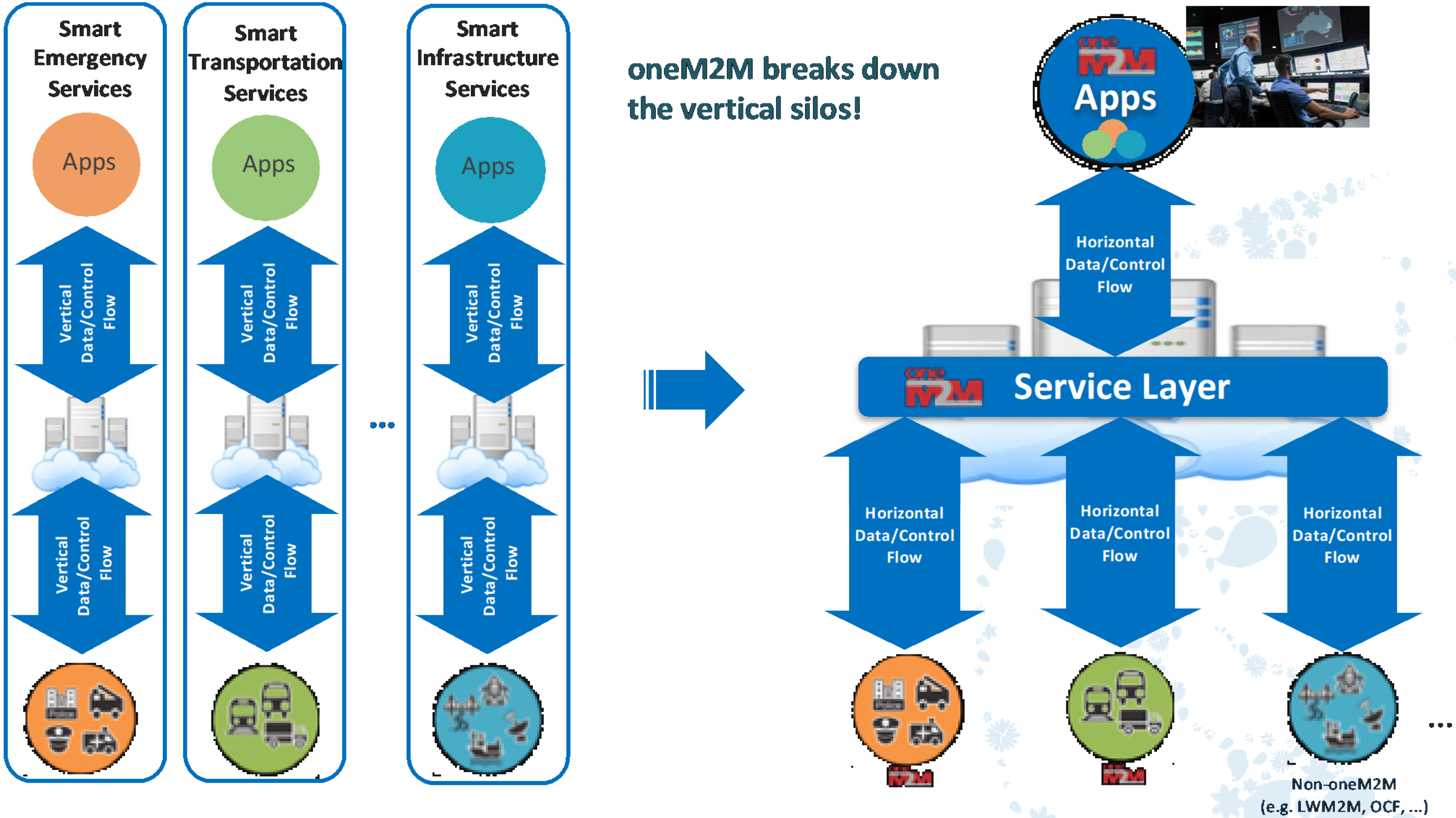
…and most importantly: oneM2M ***is a Global Standard – not controlled by a single private company!***

OneM2M



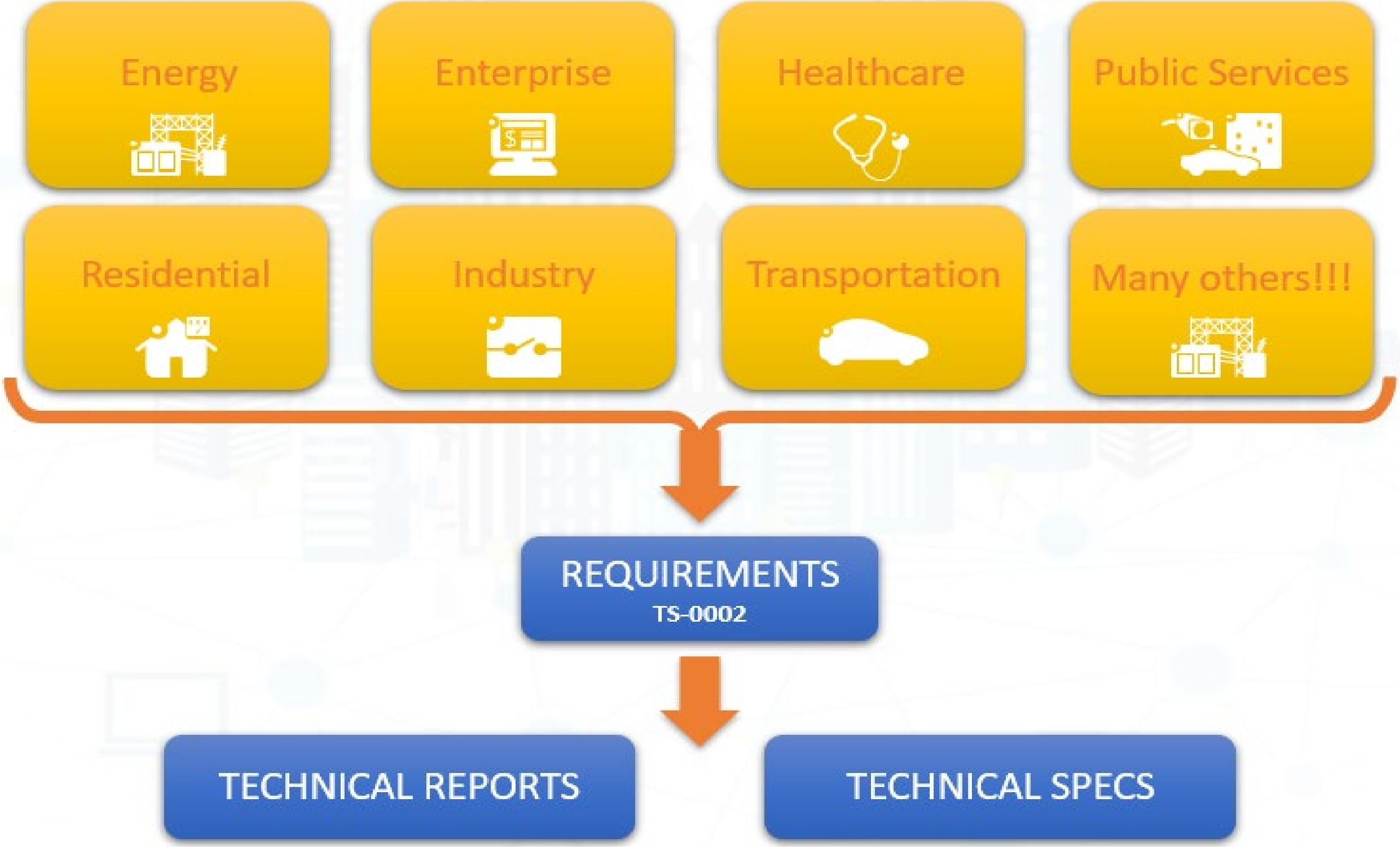
- oneM2M standard is based on a “Store and Share” resource REST based paradigm.
- The data may be made available in the platform to the other applications, interested application are notified by means of subscription.
- Privacy is ensured by a strict Access Control Management, which relies on underlying 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 frameworf designed to connect the different IoT technologies.

oneM2M integrates the vertical silos!


Smart Emergency Services
Apps
Vertical Data/Control Flow
Vertical Data/Control Flow
Smart Transportation Services
Apps
Vertical Data/Control Flow
Vertical Data/Control Flow
…
Smart Infrastructure Services
Apps
Vertical Data/Control Flow
Vertical Data/Control Flow
oneM2M
Apps
Horizontal Data/Control Flow
oneM2M Service Layer
Horizontal Data/Control Flow
Horizontal Data/Control Flow
Horizontal Data/Control Flow
oneM2M
oneM2M
…
Non-oneM2M
(e.g. LWM2M, OCF, …)

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

Device Configuration
TS-0022

Security Solutions
TS-0003

MEF & MAF interfaces
TS-0032

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

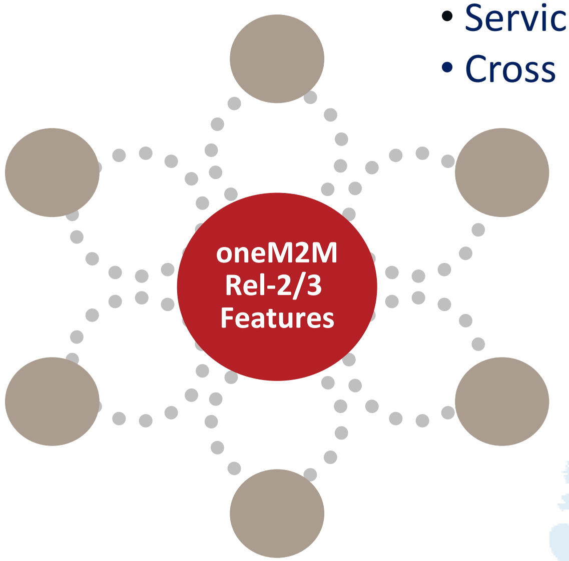
- Home Appliance Information Models & SDT
- Mapping to existing standards (OCF, ECHONET, GoTAPI...)

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

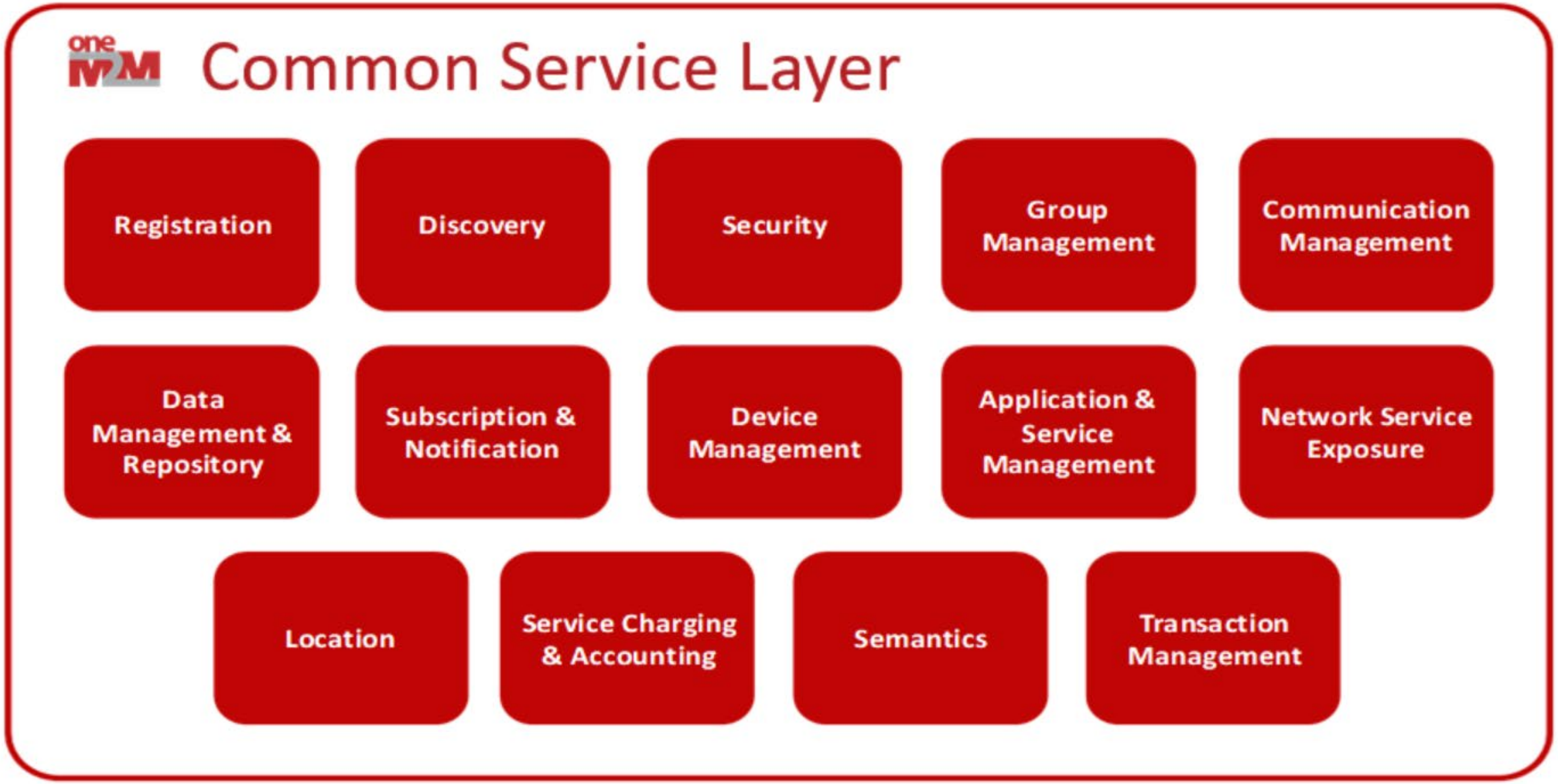
oneM2M as generic interworking framework

- 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

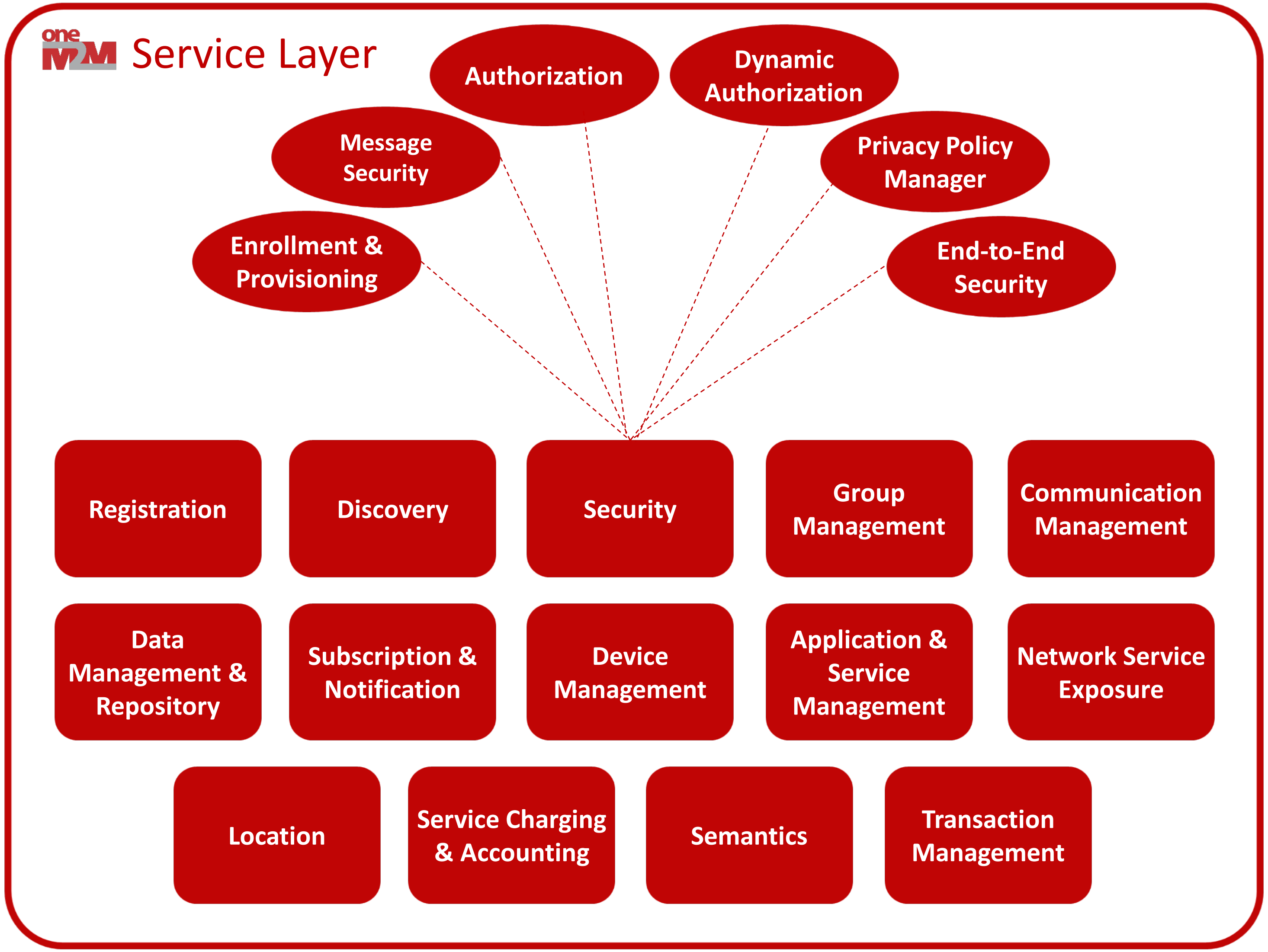
oneM2M Functions provided to applications.



Common Service Layer

- Registration
- Discovery
- Security
- Group Management
- Communication Management
- Data Management & Repository
- Subscription & Notification
- Device Management
- Application & Service Management
- Network Service Exposure
- Location
- Service Charging & Accounting
- Semantics
- Transaction Management

oneM2M Security Framework



oneM2M compliments existing proven security technologies to address IoT Security challenges.

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:

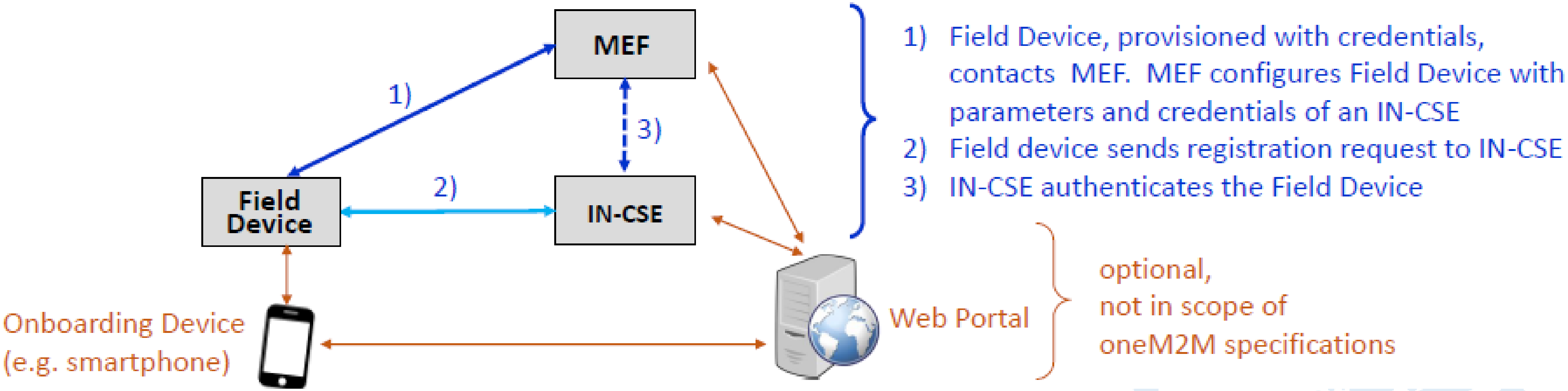
- Identity protection
  - Capability to use pseudonyms to protect anonymity of transactions.
- Sensitive data handling
  - Capability to protect sensitive data (e.g. local credentials) and functions (e.g. data encryption/decryption) in a Secure Environment (e.g. Smart Card or Virtual Smart Cart)
- Security 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



1) Field Device, provisioned with credentials, contacts MEF. MEF configures Field Device with parameters and credentials of an IN-CSE
2) Field device sends registration request to IN-CSE
3) IN-CSE authenticates the Field Device

optional,
not in scope of
oneM2M specifications

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)

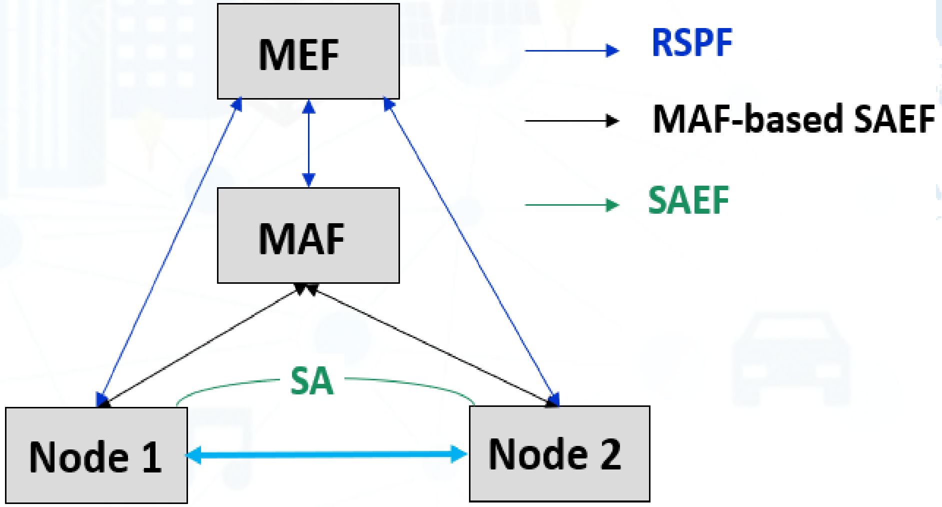
M2M Enrolment Function allows 3 types of Remote Security Provisioning Frameworks (RSPF)

- 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)

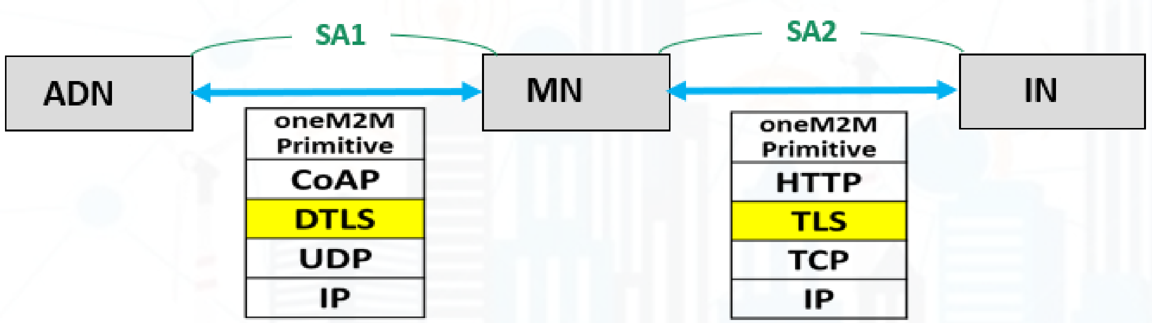
MEF can trigger the Field Device to execute a variety of procedures, inc

- Configuration of Field devices with registration parameters and authen operational Security Frameworks (see next slide)
- Provisioning of symmetric key credentials
- Provisioning of certificates (certificate (re-)enrolment using EST and S recommendations)

MEF is operated by M2M Service Provider or trusted 3rd party (device r operator) Z



Message Security between adjacent Entities: The operational security framework



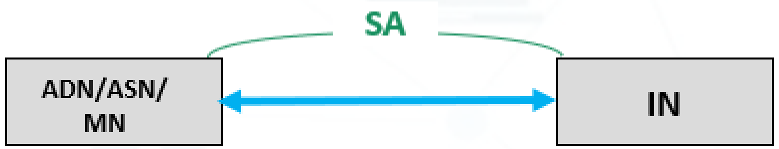
Message Security between adjacent Entities: The operational security framework

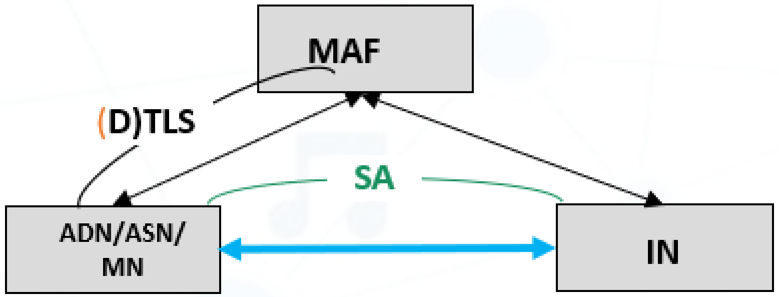
Uses (Datagram) Transport Layer Security Protocols, TLS/DTLS Version 1.2

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

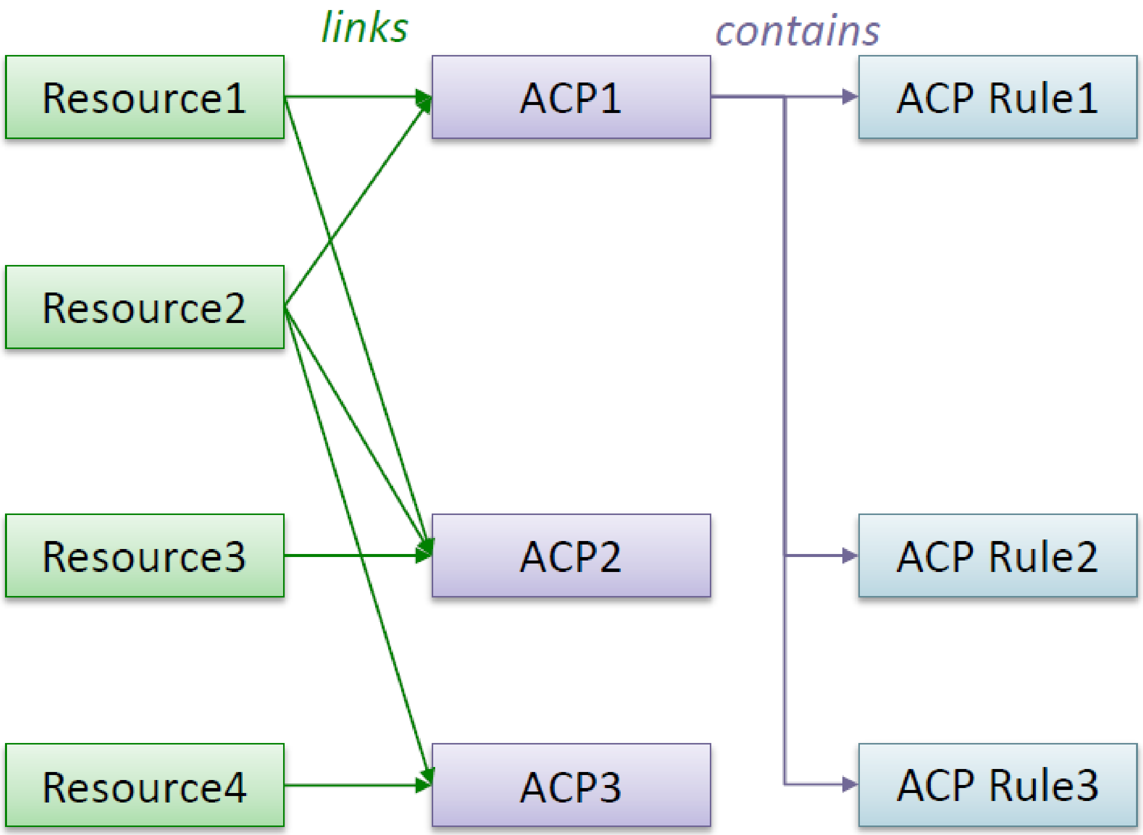
oneM2M is based on a RESTful architecture

- 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



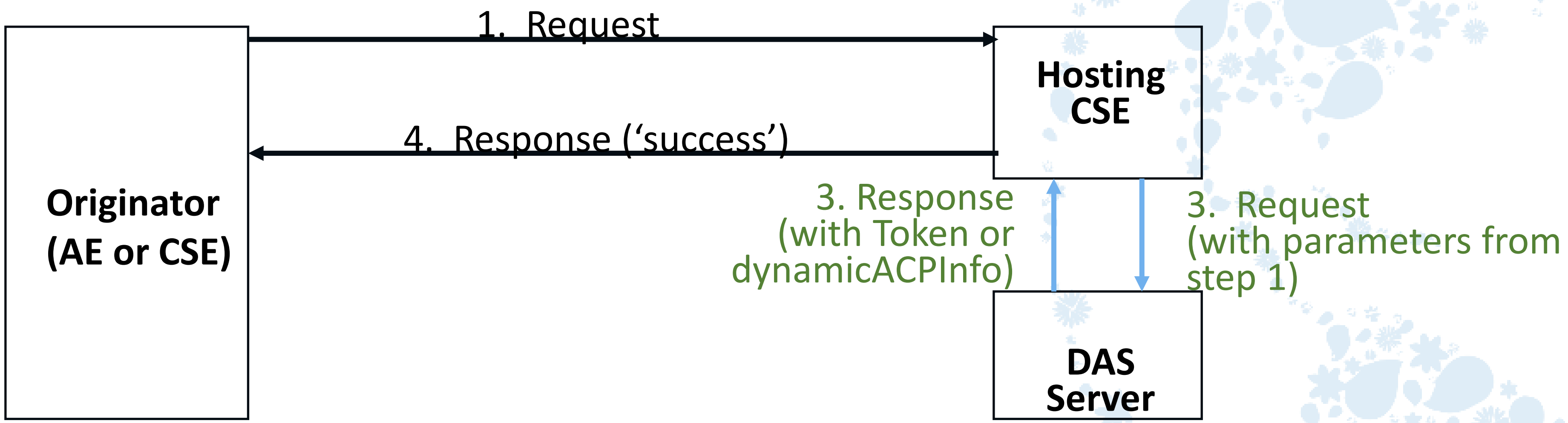
Resource access is authorized based upon satisfying at least on Access Control Policy (ACP) rule in one of the linked ACPs.

Dynamic Authorization

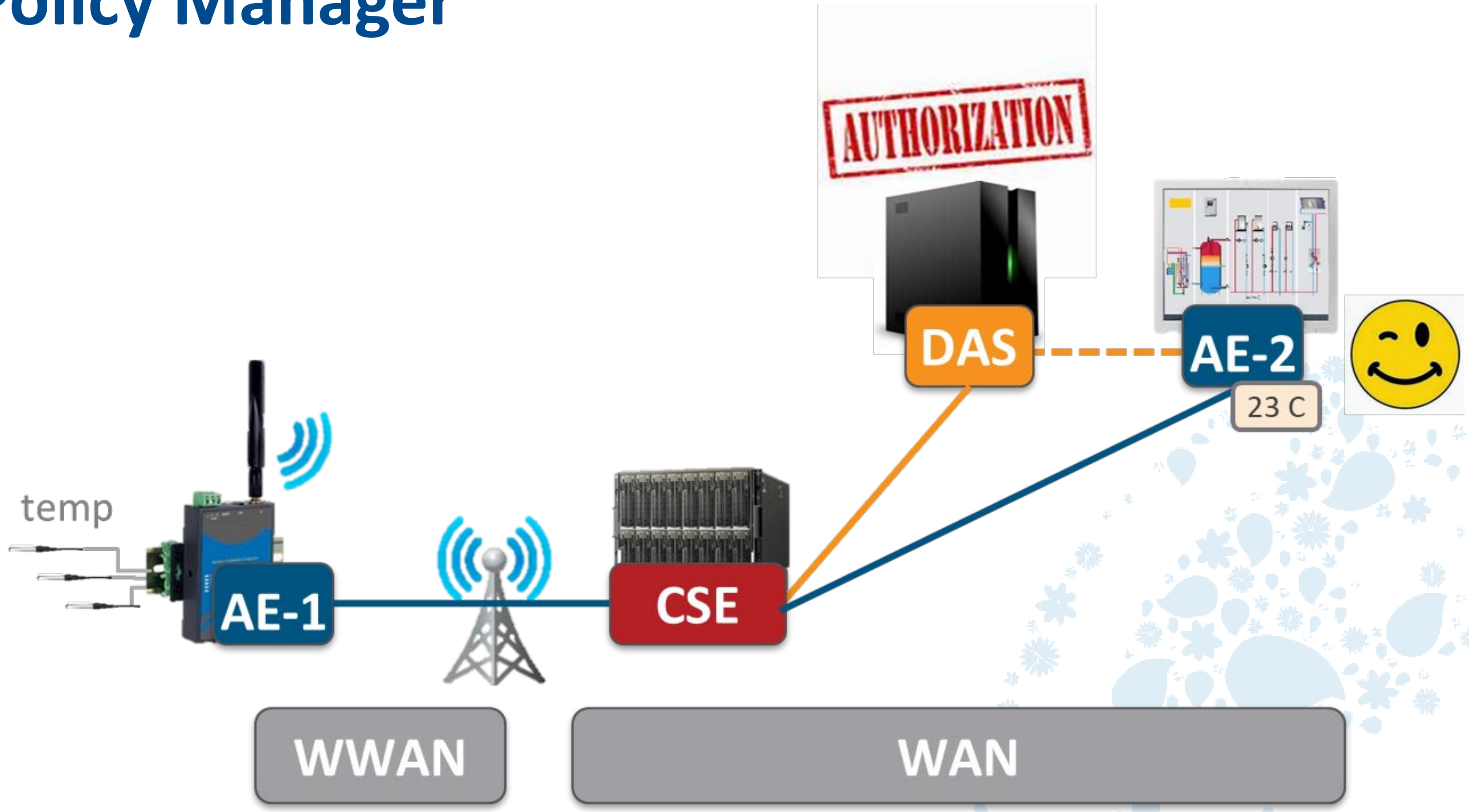
Dynamic Authorization: Originator or Hosting CSE requesting authorization of Originator – provided by a Dynamic Authorization System (DAS) Server

- 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


1. Request
Hosting CSE
4. Response ('success')
Originator (AE or CSE)
3. Response (with Token or dynamicACPInfo)
3. Request (with parameters from step 1)
DAS Server

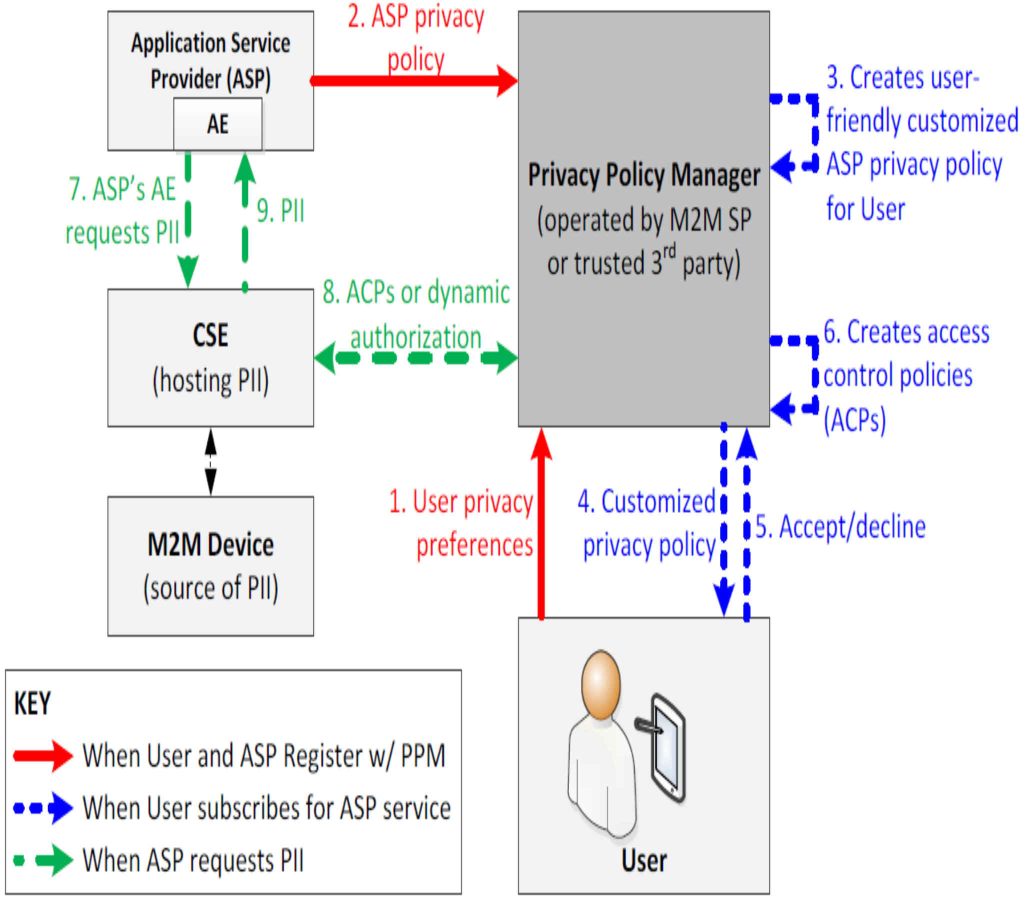
Privacy Policy Manager



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

Privacy Policy Manager (PPM)

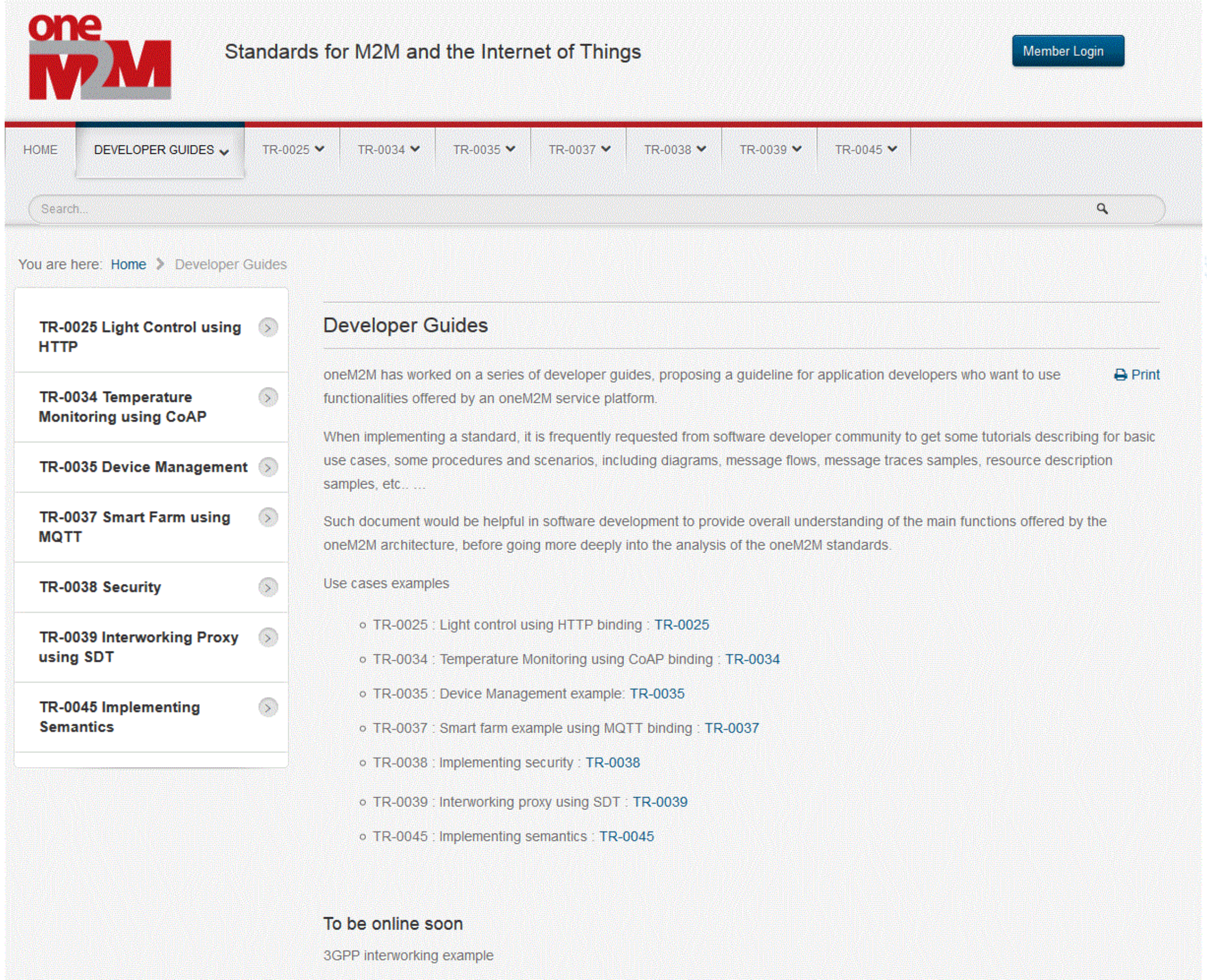
- The PPM is a personal data management framework
- The PPM converts a User's privacy preferences into access control information in order to protect the User's Personally Identifiable Information (PII) from access by unauthorized parties.
- Access control information consists of static and dynamic access 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


Application Service Provider (ASP)
AE
2. ASP privacy policy
Privacy Policy Manager (operated by M2M SP or trusted 3rd party)
3. Creates user-friendly customized ASP privacy policy for User
7. ASP's AE requests PII
9. PII
8. ACPs or dynamic authorization
CSE (hosting PII)
6. Creates access control policies (ACPs)
M2M Device (source of PII)
1. User privacy preferences
4. Customized privacy policy
5. Accept/decline
User
KEY
When User and ASP Register w/ PPM
When User subscribes for ASP service
When ASP requests PII

Publicly Accessible Links

Developer Guides

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



You are here: Home > Developer Guides

- TR-0025 Light Control using HTTP
- TR-0034 Temperature Monitoring using CoAP
- TR-0035 Device Management
- TR-0037 Smart Farm using MQTT
- TR-0038 Security
- TR-0039 Interworking Proxy using SDT
- TR-0045 Implementing Semantics

Developer Guides

oneM2M has worked on a series of developer guides, proposing a guideline for application developers who want to use functionalities offered by an oneM2M service platform.

When implementing a standard, it is frequently requested from software developer community to get some tutorials describing for basic use cases, some procedures and scenarios, including diagrams, message flows, message traces samples, resource description samples, etc.. ...

Such document would be helpful in software development to provide overall understanding of the main functions offered by the oneM2M architecture, before going more deeply into the analysis of the oneM2M standards.

Use cases examples

- TR-0025 : Light control using HTTP binding : TR-0025
- TR-0034 : Temperature Monitoring using CoAP binding : TR-0034
- TR-0035 : Device Management example: TR-0035
- TR-0037 : Smart farm example using MQTT binding : TR-0037
- TR-0038 : Implementing security : TR-0038
- TR-0039 : Interworking proxy using SDT : TR-0039
- TR-0045 : Implementing semantics : TR-0045

To be online soon

3GPP interworking example

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