



Security Conference

Security in oneM2M

Presented by:

Rana Kamill

IoT Ecosystems Architecture Solution Manager, BT

Senior Representative, oneM2M.



18/10/2023



About the oneM2M global partnership

A global partnership among SDOs and Industry Associations/Fora

Main goal: create consistency in how devices, servers and applications communicate through a standardized M2M Service Layer

- Interoperability
- Cost-effectiveness / economies of scale
- Reduced fragmentation
- Larger market

Open and transparent: all working documents are public.

All deliverables available free of charge

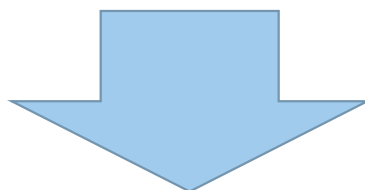
Builds on use cases and requirements from industry sectors

Detailed scope at <http://www.onem2m.org/>



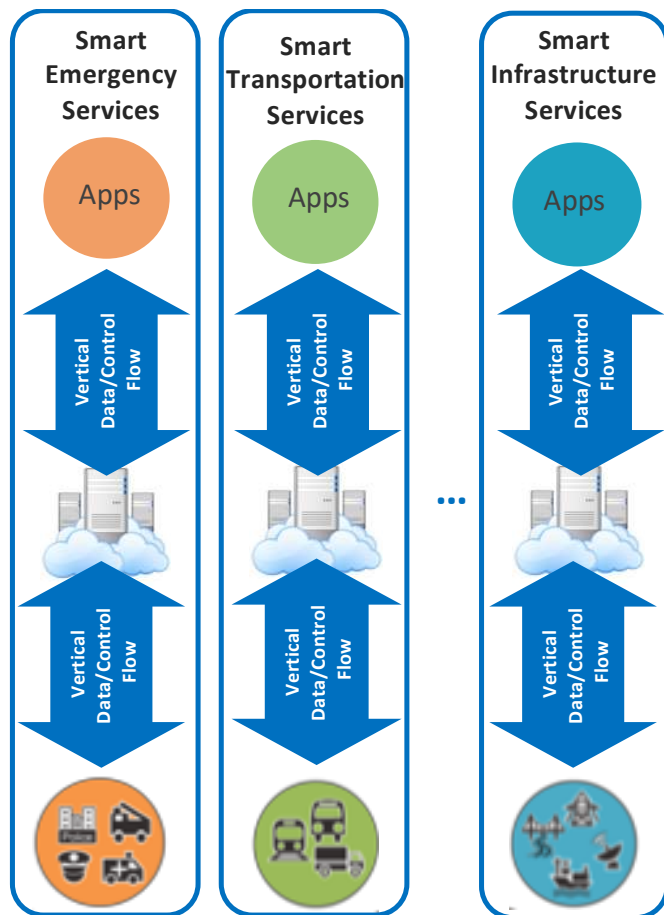
Opportunities and problems

- **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.

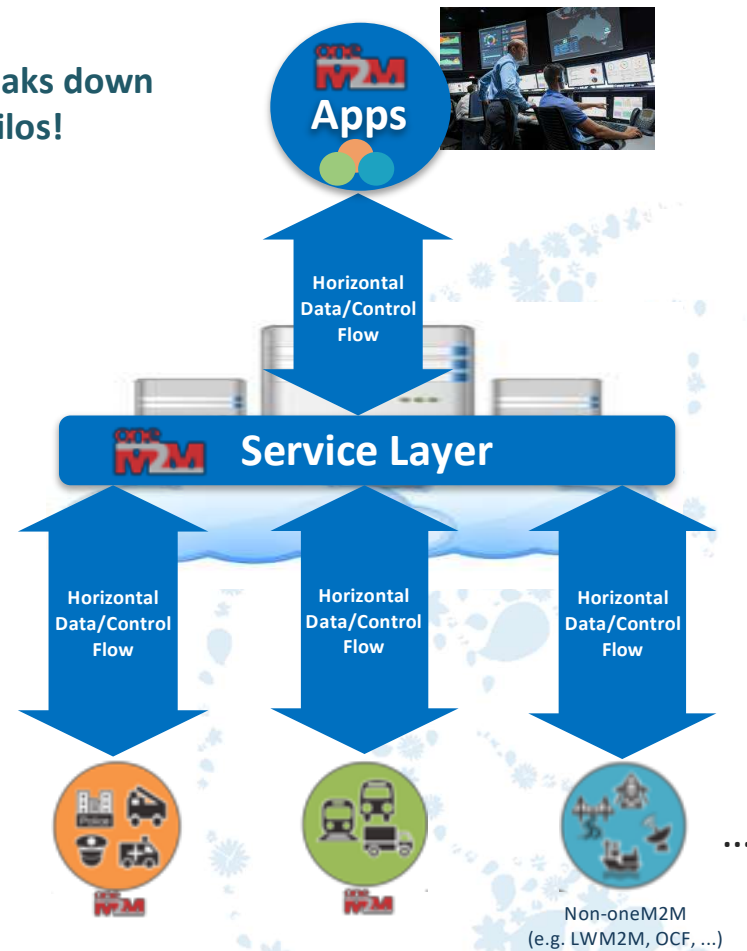
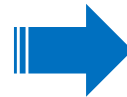


- **Simplify** the environment, remove the unnecessary duplicated solutions (economy of scale), **preserve** the necessary/opportune solution specialization by **interworking**.

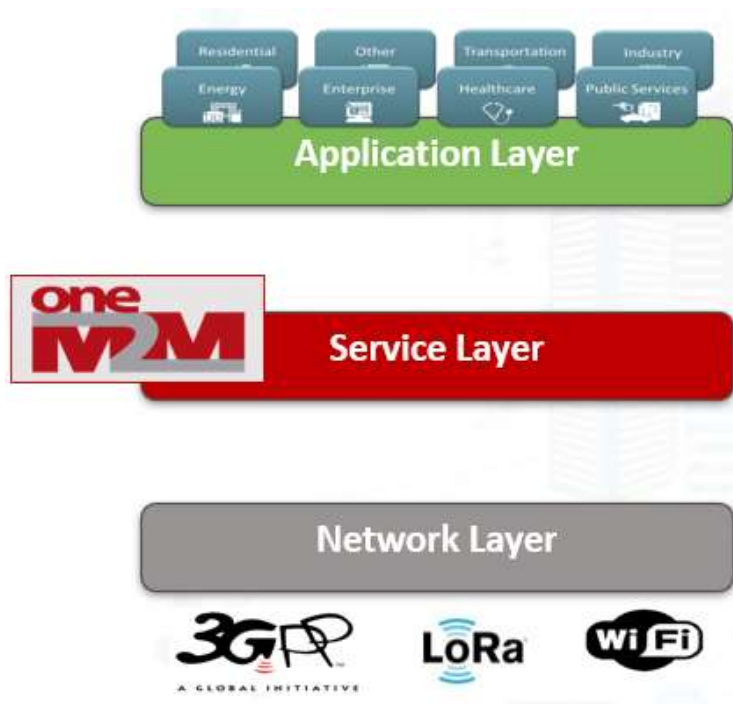
oneM2M integrates the vertical silos!



oneM2M breaks down the vertical silos!



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:



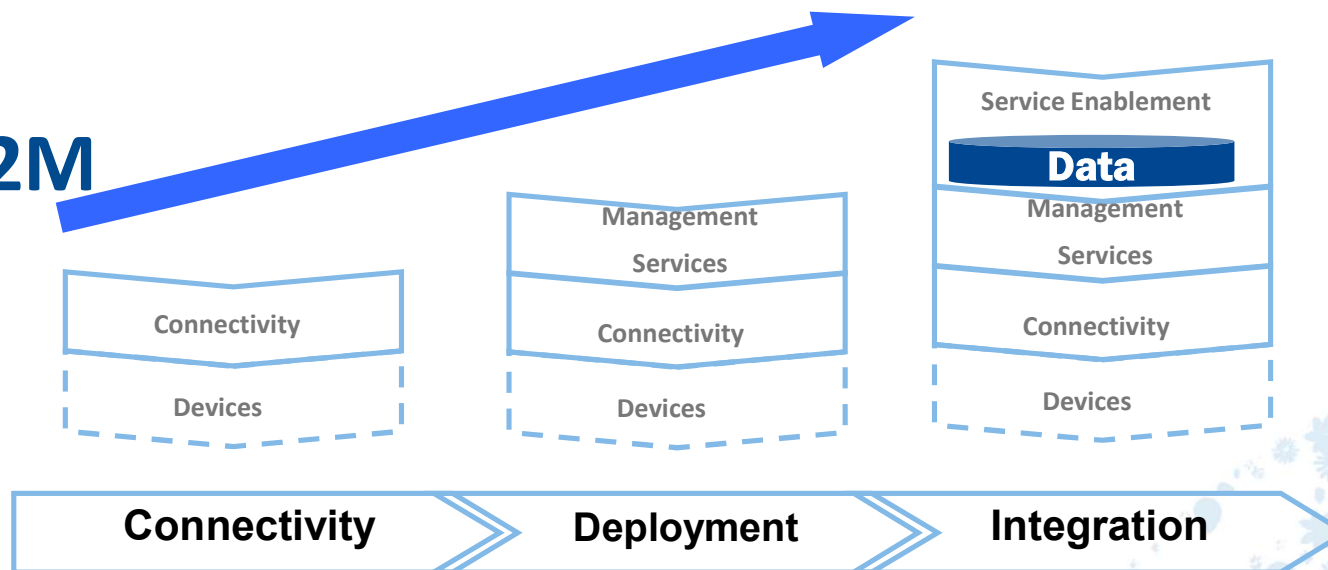
*is a **Global Standard** – not controlled by a single private company!*

Why use oneM2M?

- The only formal standard 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**
- **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
- **Simple** if you use the core functions and know your deployment architecture

oneM2M

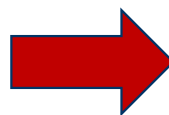


- ▶ oneM2M standard is based on a “Store and Share” resource REST based paradigm.
- ▶ The data may be made available in the platform to the other applications, interested application are notified by means of subscription.
- ▶ Privacy is ensured by a strict Access Control Management.
- ▶ oneM2M is heavily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

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)**

Security in oneM2M

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 Card)
- Security administration (related to device management)
 - Creates and administers dedicated Secure Environments and post-provisioning of master credentials.

Security in oneM2M

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

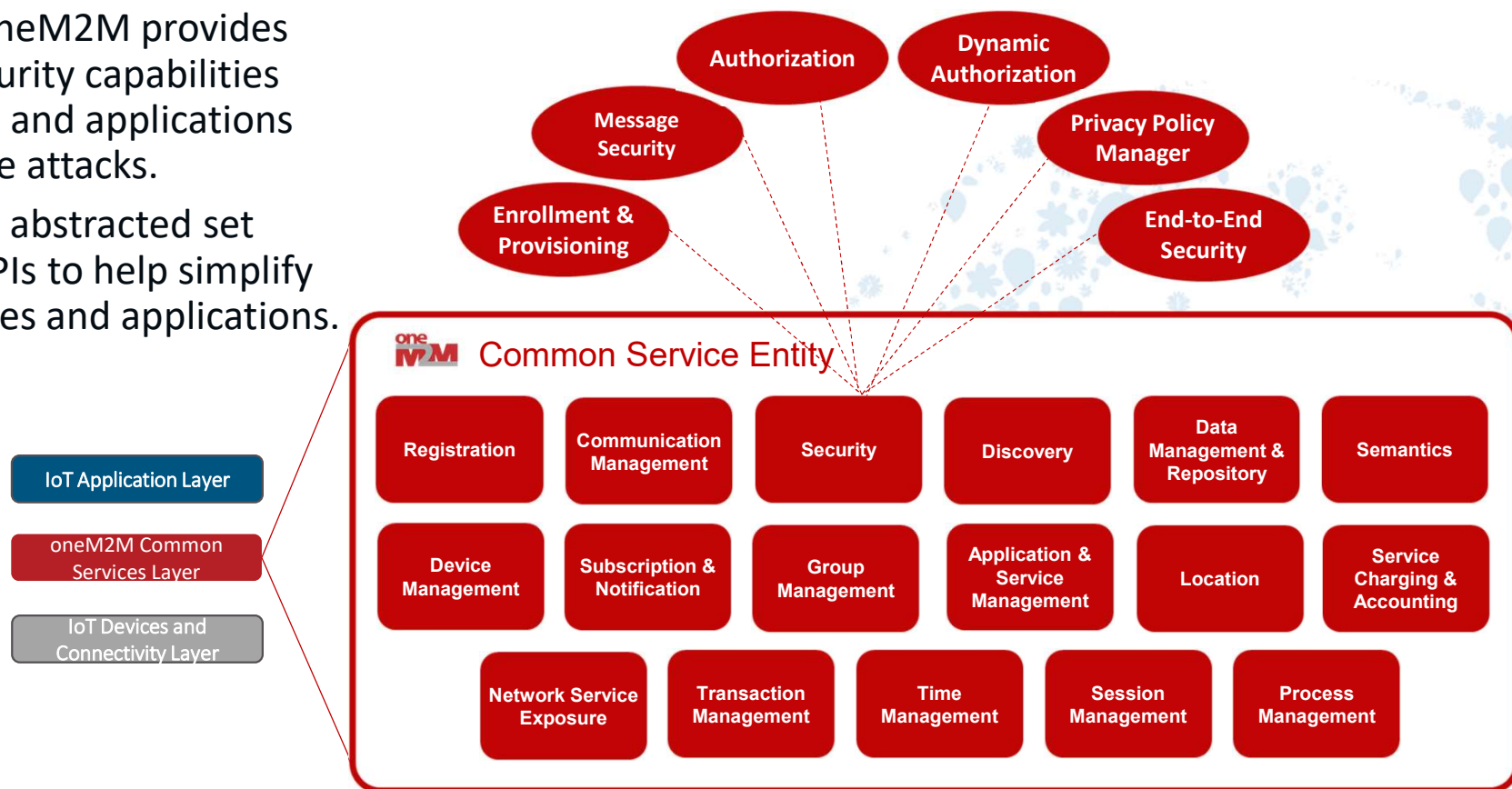
- Expose common services to applications, depending on implementation.
- Provide common interface for remote security administration, if needed.

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.

oneM2M Security Framework

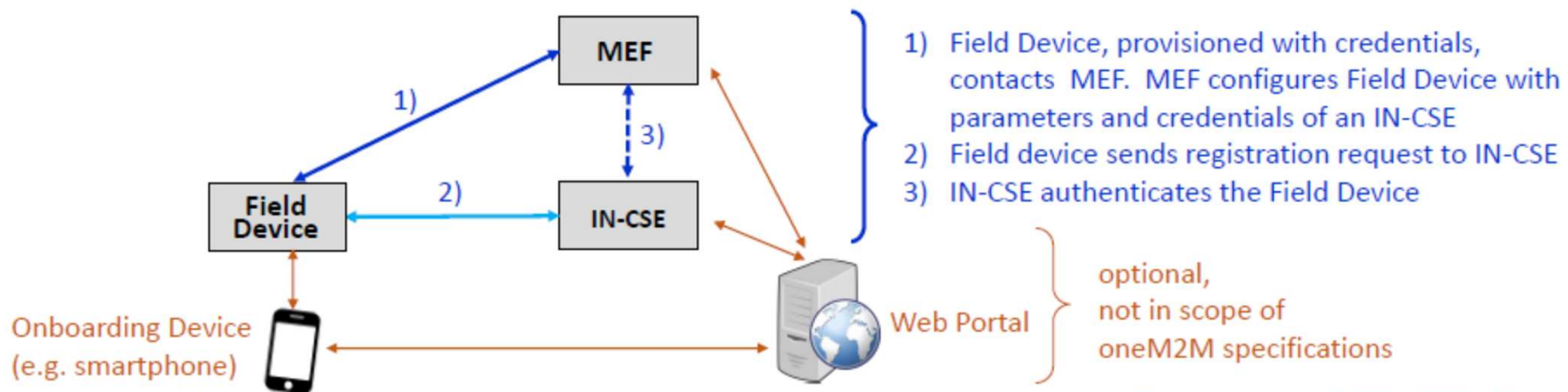
- oneM2M provides a Common Services "Toolkit"
- Within this toolkit, oneM2M provides a common set of security capabilities to secure IoT devices and applications and prevent/mitigate attacks.
- oneM2M exposes an abstracted set of security related APIs to help simplify security for IoT devices and applications.



Enrolment & 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



Enrolment & Provisioning (Onboarding)

MEF supports 3 types of 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)

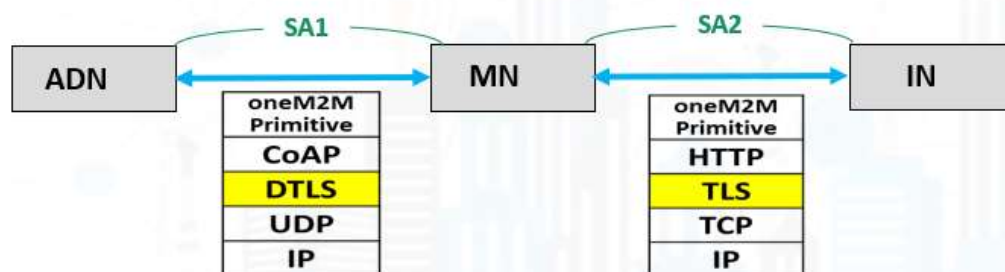
MEF can trigger the Field Device to execute a variety of procedures, including the matching

- Configuration of Field devices with registration parameters and authentication profiles applicable to the operational Security Frameworks
- Provisioning of symmetric key credentials
- Provisioning of certificates (certificate (re-)enrolment using EST and SCEP specified by IETF recommendations)

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.

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

Message Security between adjacent Entities: The operational security framework



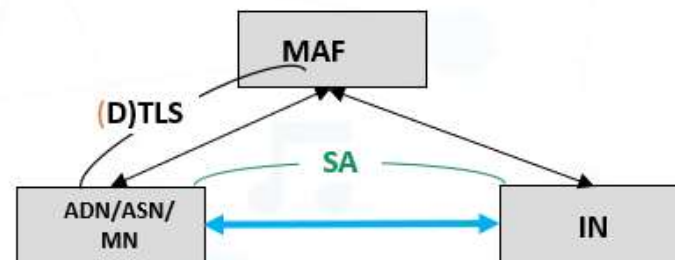
Message Security between adjacent Entities:
The operational security framework

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

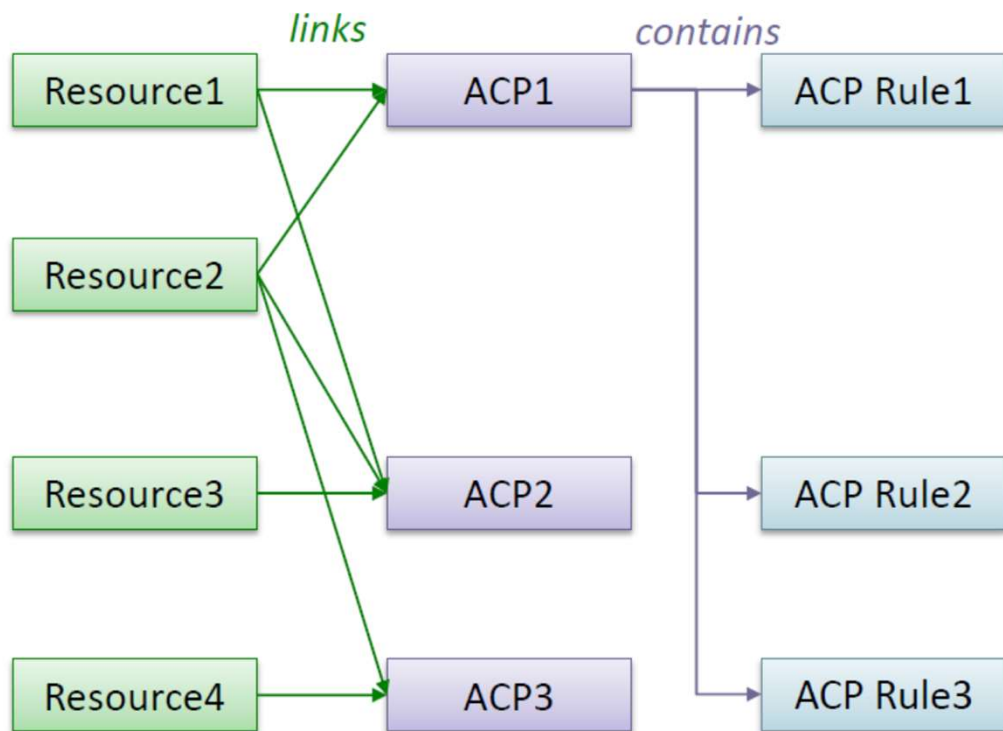
oneM2M is based on a RESTful architecture

- 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



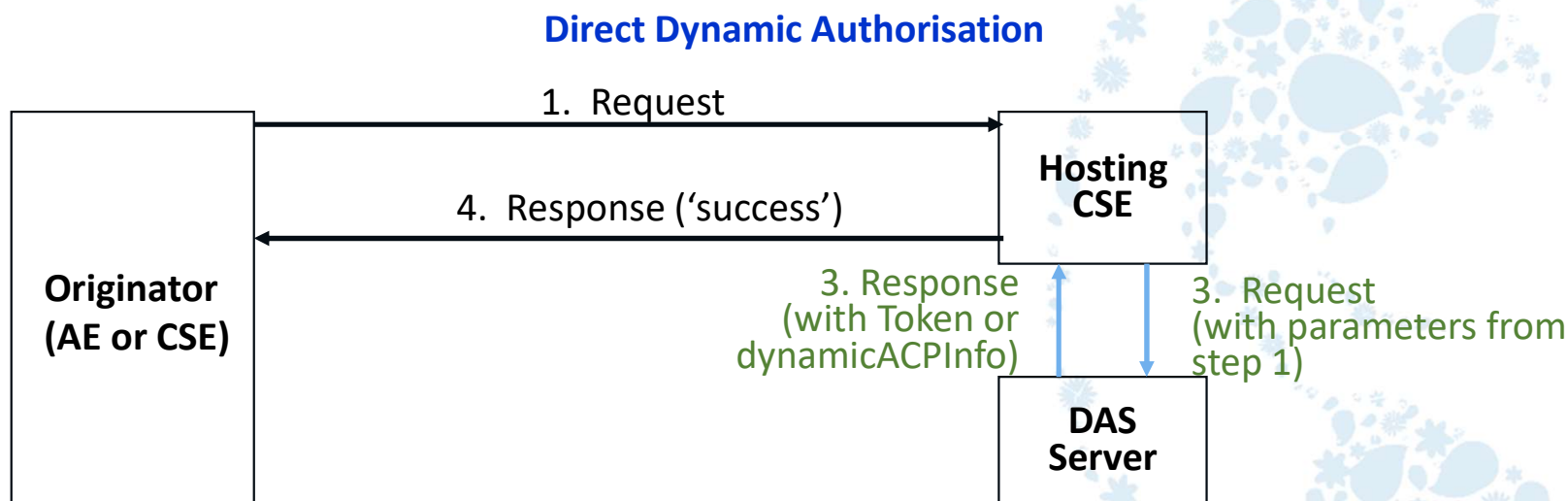
Resource access is authorized based upon satisfying at least one Access Control Policy (ACP) rule in one of the linked ACPs.



Dynamic Authorization

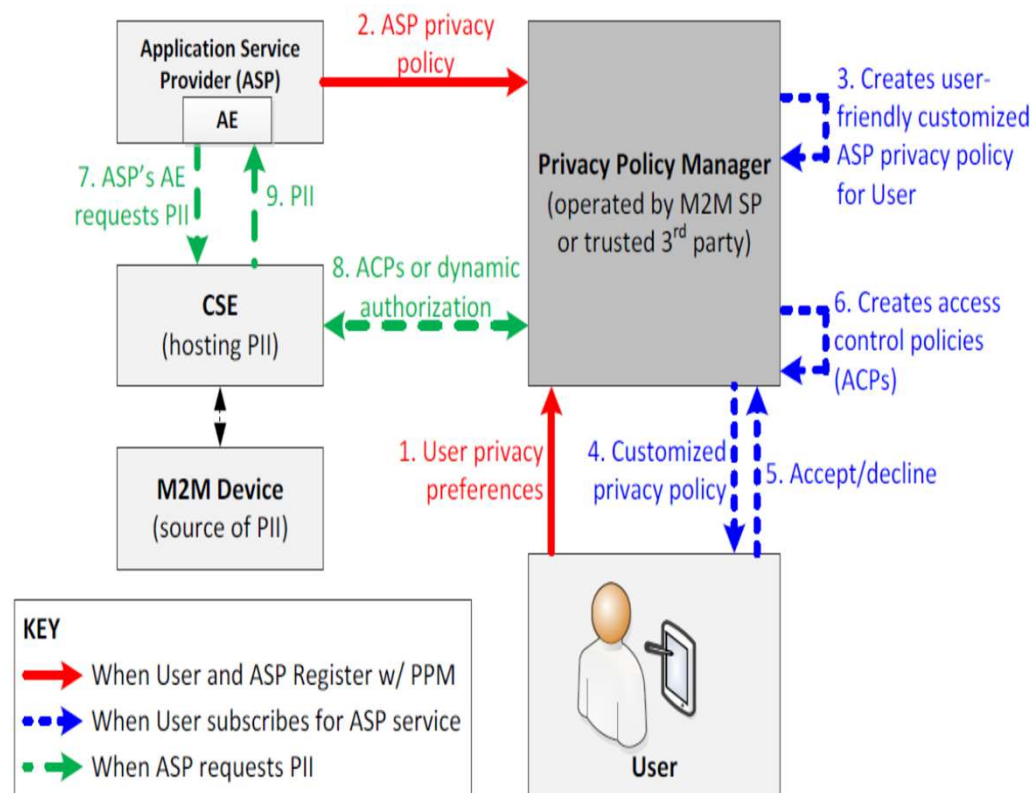
Dynamic Authorization: Originator or Hosting CSE requesting authorization of Originator – provided by a Dynamic Authorization System (DAS) Server

- 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)



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 Conditions Markup language" to derive consensus between the User's privacy preferences and an Application Service Provider's privacy policies



Support to developers and users

The community strives to ease access to the oneM2M world. It has developed abundant material to that effect:

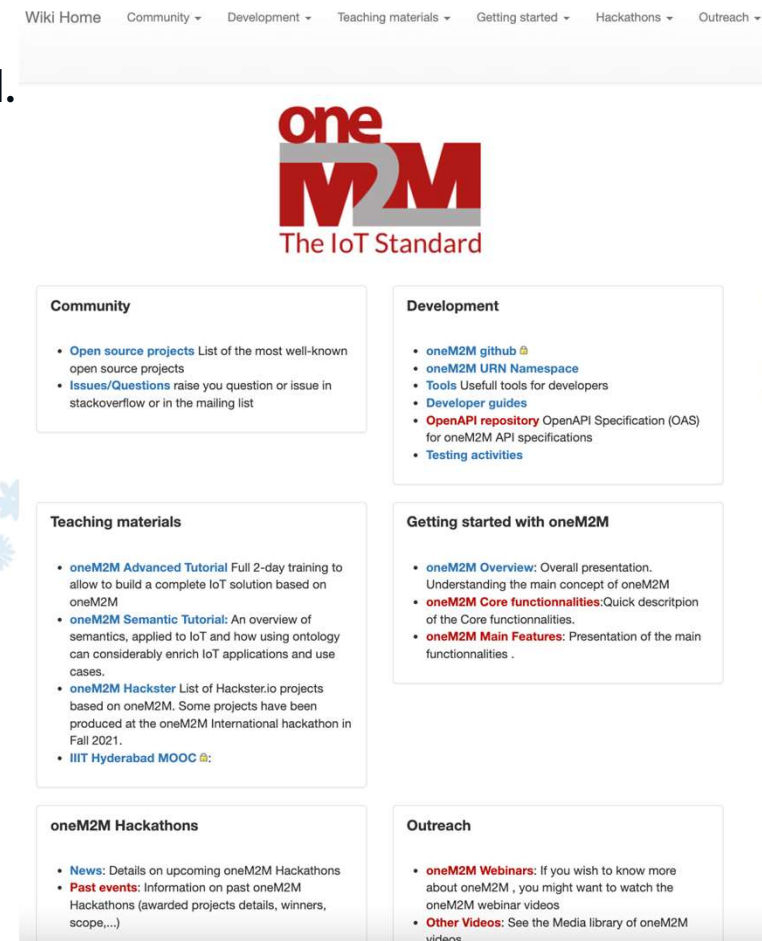
- Developer Guides
- Video Tutorials
- Wiki

oneM2M also organizes events to support implementers and developers as well as to create awareness in the academic world:

- Tutorials & developer events
- Hackathons
- Interoperability events

This content is freely available at the oneM2M developer resources page:

https://wiki.onem2m.org/index.php?title=Main_Page



The screenshot shows the oneM2M developer resources page. At the top, there is a navigation menu with links: Wiki Home, Community, Development, Teaching materials, Getting started, Hackathons, and Outreach. Below the menu is the oneM2M logo, which consists of the text "one" in red above "M2M" in a larger, bold red font, with "The IoT Standard" written below it. The main content area is divided into several sections, each with a title and a list of resources:

- Community**
 - **Open source projects** List of the most well-known open source projects
 - **Issues/Questions** raise you question or issue in stackoverflow or in the mailing list
- Development**
 - **oneM2M github**
 - **oneM2M URN Namespace**
 - **Tools** Useful tools for developers
 - **Developer guides**
 - **OpenAPI repository** OpenAPI Specification (OAS) for oneM2M API specifications
 - **Testing activities**
- Teaching materials**
 - **oneM2M Advanced Tutorial** Full 2-day training to allow to build a complete IoT solution based on oneM2M
 - **oneM2M Semantic Tutorial:** An overview of semantics, applied to IoT and how using ontology can considerably enrich IoT applications and use cases.
 - **oneM2M Hackster** List of Hackster.io projects based on oneM2M. Some projects have been produced at the oneM2M International hackathon in Fall 2021.
 - **IIIT Hyderabad MOOC**
- Getting started with oneM2M**
 - **oneM2M Overview:** Overall presentation. Understanding the main concept of oneM2M
 - **oneM2M Core functionalities:** Quick description of the Core functionalities.
 - **oneM2M Main Features:** Presentation of the main functionalities .
- oneM2M Hackathons**
 - **News:** Details on upcoming oneM2M Hackathons
 - **Past events:** Information on past oneM2M Hackathons (awarded projects details, winners, scope...)
- Outreach**
 - **oneM2M Webinars:** If you wish to know more about oneM2M , you might want to watch the oneM2M webinar videos
 - **Other Videos:** See the Media library of oneM2M videos

Thank You!

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