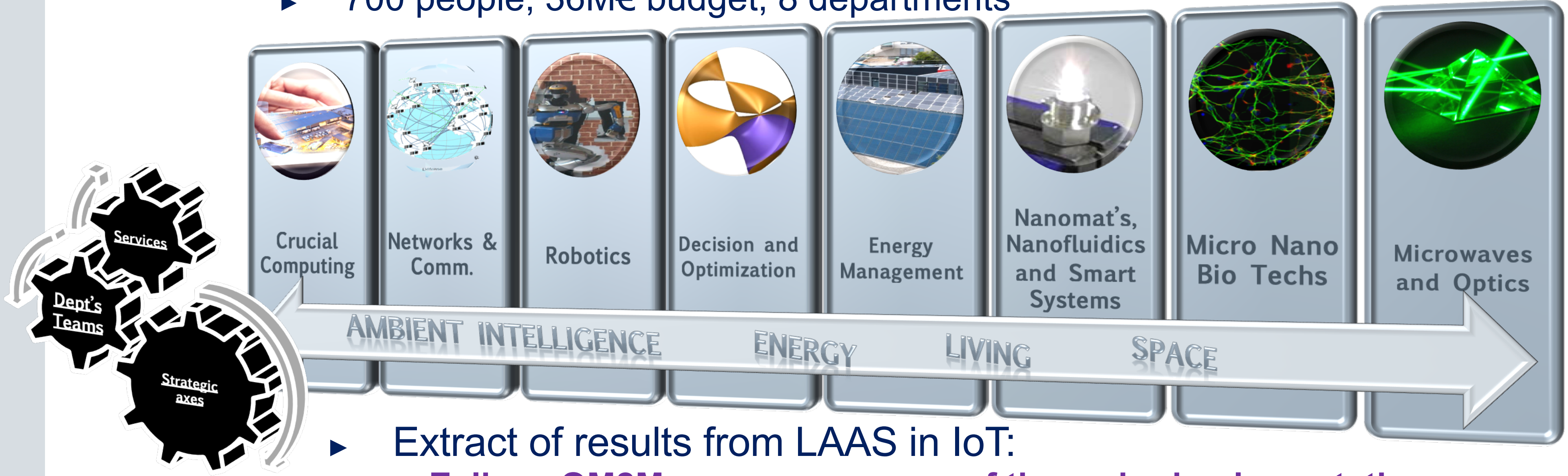
oneM2M Service, Data and Security

Thierry Monteil – **monteil@laas.fr** (Professor at INSA – Univ. of Toulouse / Researcher at LAAS-CNRS)

LAAS-CNRS - Laboratory for Analysis and Architecture of Systems

- ICT domain
- 700 people, 36M€ budget, 8 departments



- Extract of results from LAAS in IoT:
  - **Eclipse OM2M opensource: one of the major implementation of oneM2M** [1]
  - **IoT-O ontology for IoT** [2]
  - **LOM2M: oneM2M for very constraint gateway (New in 2019)** [3]
  - **Autonomic system for IoT and fog computing** [4]

OM2M Connecting things

[1] S. Sicari, A. Rizzardi, L. Alfredo, T. Monteil and A. Coen-Porisini, Secure OM2M Service Platform, Self-IoT - IEEE International Conference on Autonomic Computing ICAC 2015.

[2] N. Seydoux, K. Drira, N. Hernandez, T. Monteil, IoT-O, a Core-Domain IoT Ontology to Represent Connected Devices Networks. International Conference on Knowledge Engineering and Knowledge Management - EKAW2016 : 561-576, Bologna, Italy, November, 2016

[3] Orange, LAAS-CNRS, pilot things, sierra wireless, Device Management of heterogeneous and constrained IoT devices using oneM2M and SDT abstraction layer,ETSI IoT Week, october 2019

[4] N. Seydoux, K. Drira, N. Hernandez, T. Monteil, Reasoning on the edge or in the cloud ?, Internet Technology Letters, avril 2018

Outline

- Internet of Things
- General information on oneM2M
- Service architecture based on REST
- Data management
  - In oneM2M
  - Ongoing research
- Security and privacy
  - In oneM2M
  - Ongoing research

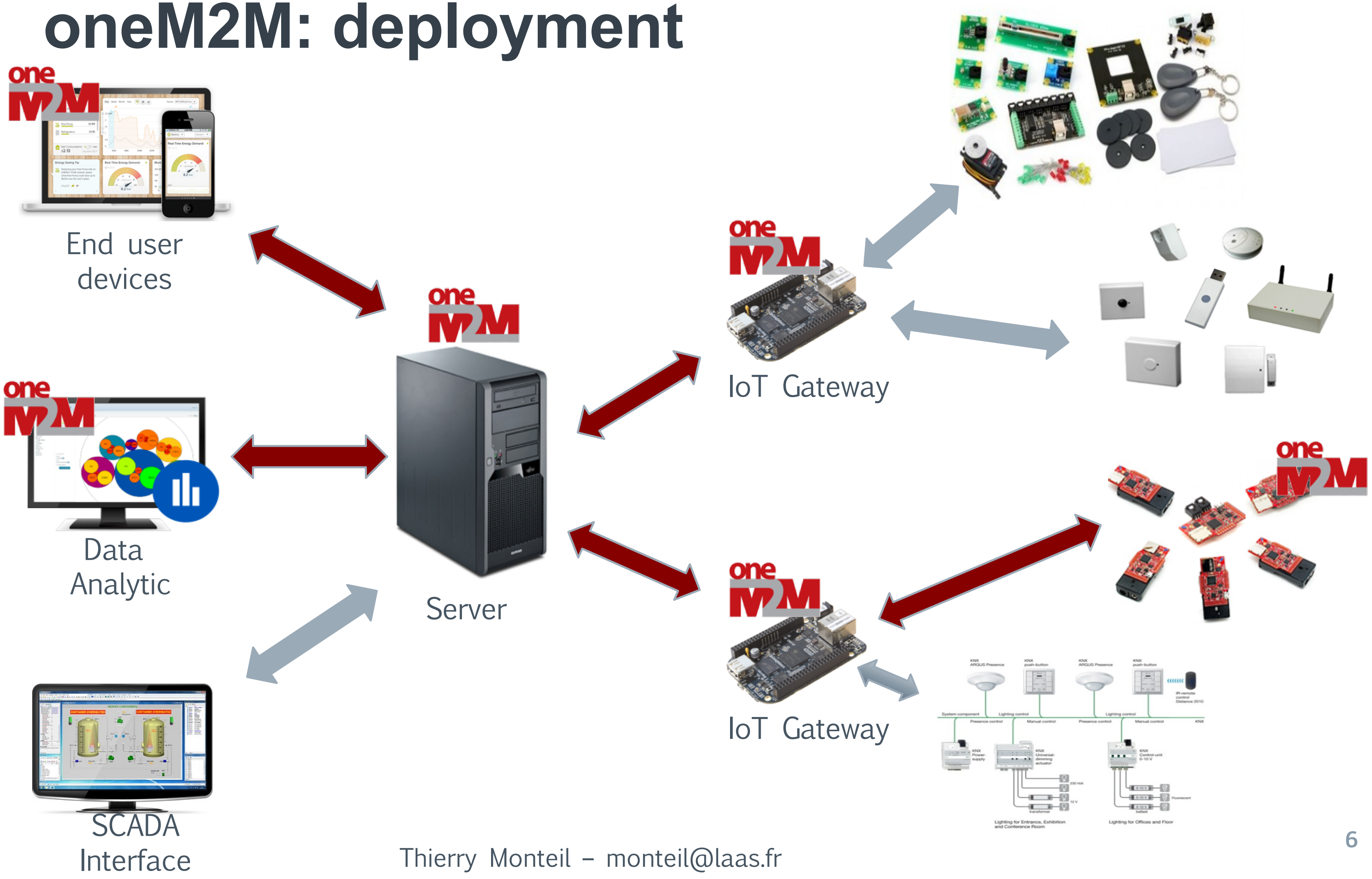
IoT service platform features

- Why do we need an IoT service platform ?
  - **Device management**
    - Device provisioning
    - Connectivity monitoring
    - Devices supervision
  - **Messages and data management**
    - Message routing
    - Data collection
    - Data storage and data history management
    - Notification management
    - Access right management
  - **Security and Privacy**
  - **Application management**
    - Tooling, SDKs, APIs
    - Rapid application development (RAD)
  - **Quality of Service for real applications**

oneM2M : interoperability by design

- Overview:
  - Generic IoT service platform, designed for multiple verticals.
- Set of standards:
  - HTTP, MQTT, CoAP, WebSocket, LWM2M, SAREF, etc.
- Interworking with other IoT platforms / Systems
  - **Interworking Proxy Entity (IPE)** to develop “translators” towards other technology/protocol/system/IoT platform:
    - OIC Interworking Proxy, AllJoyn Interworking Proxy
    - 3GPP (5G)
    - oneM2M Release 2 & 3:
      - Generic IPE (Ontology-based Interworking)
      - IoT proximal Interworking TS-0033
  - **FlexContainer** to ease data exchange between different platforms.
  - **Semantics** support.
- Implementation availability
  - Both open source and vendor specific implementations exist.

oneM2M: deployment



End user devices

Data Analytic

SCADA Interface

Server

IoT Gateway

IoT Gateway

oneM2M: Architecture[1]

From oneM2M Service Layer Platform – Initial Release: **Omar Elloumi/Nicolas Damour**

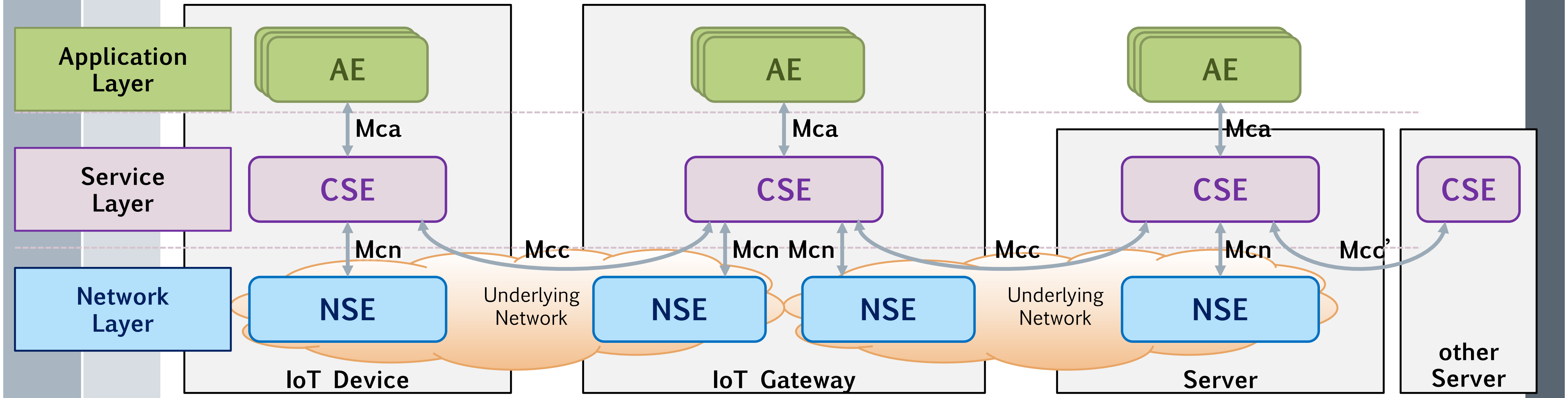
Reference Point One or more interfaces - **Mca**, **Mcn**, **Mcc** and **Mcc'** (between 2 service providers)

Common Services Entity Provides the set of "service functions" that are common to the M2M environments

Application Entity Provides application logic for the end-to-end M2M solutions

Network Services Entity Provides services to the CSEs besides the pure data transport

Node Logical equivalent of a physical (or possibly virtualized, especially on the server side) device



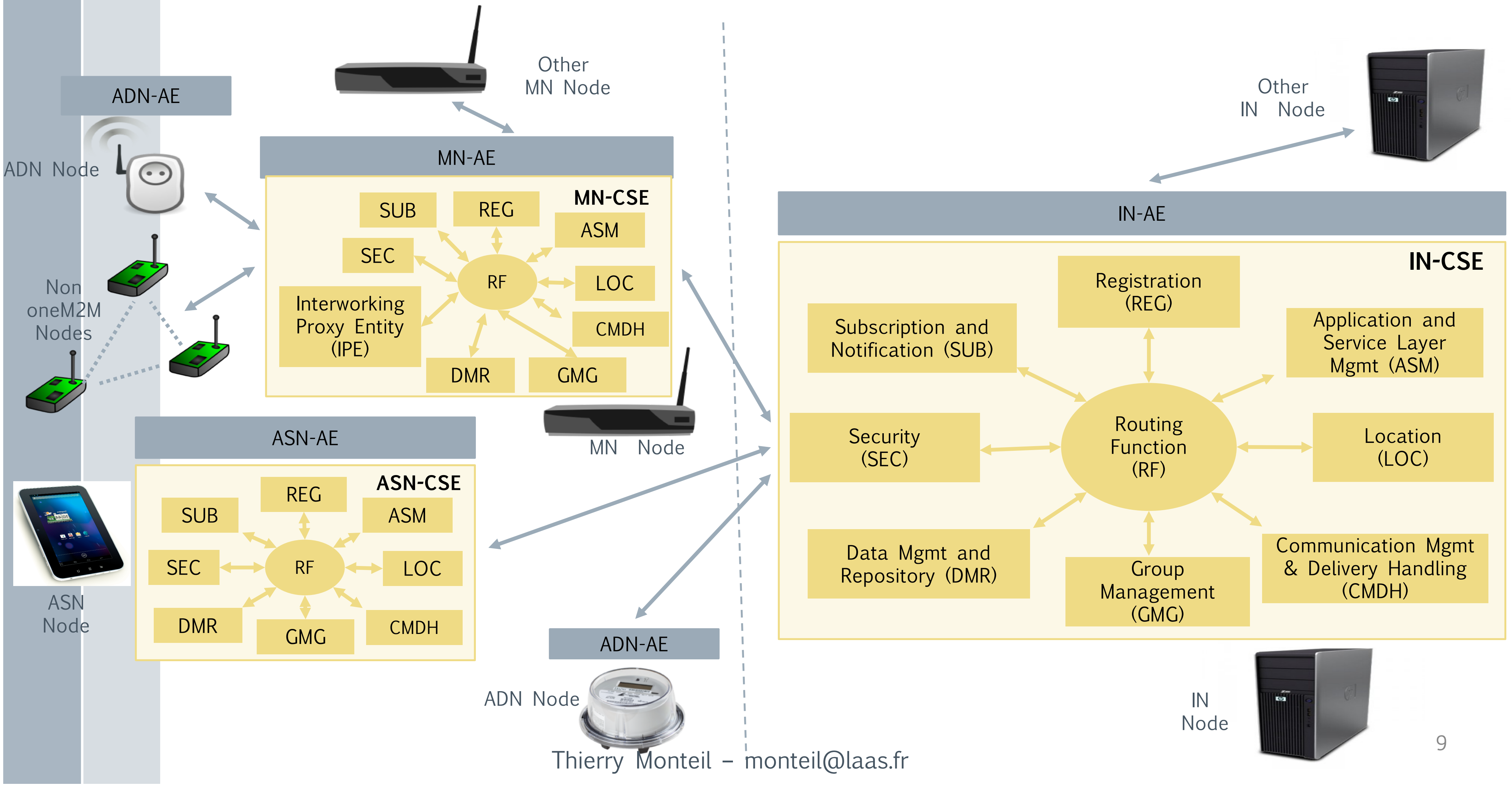
[1] Onem2m.org, TS-0001 Functional Architecture

oneM2M: Common Service Functions

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

From oneM2M Service Layer Platform – Initial Release: **Omar Elloumi / Nicolas Damour**

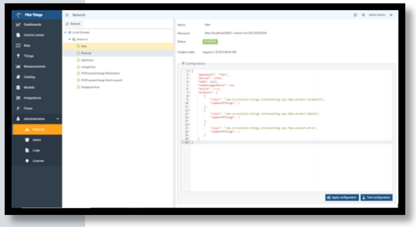
Interoperability: Standardized OneM2M Service



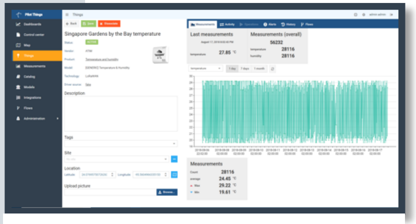
Real Deployment

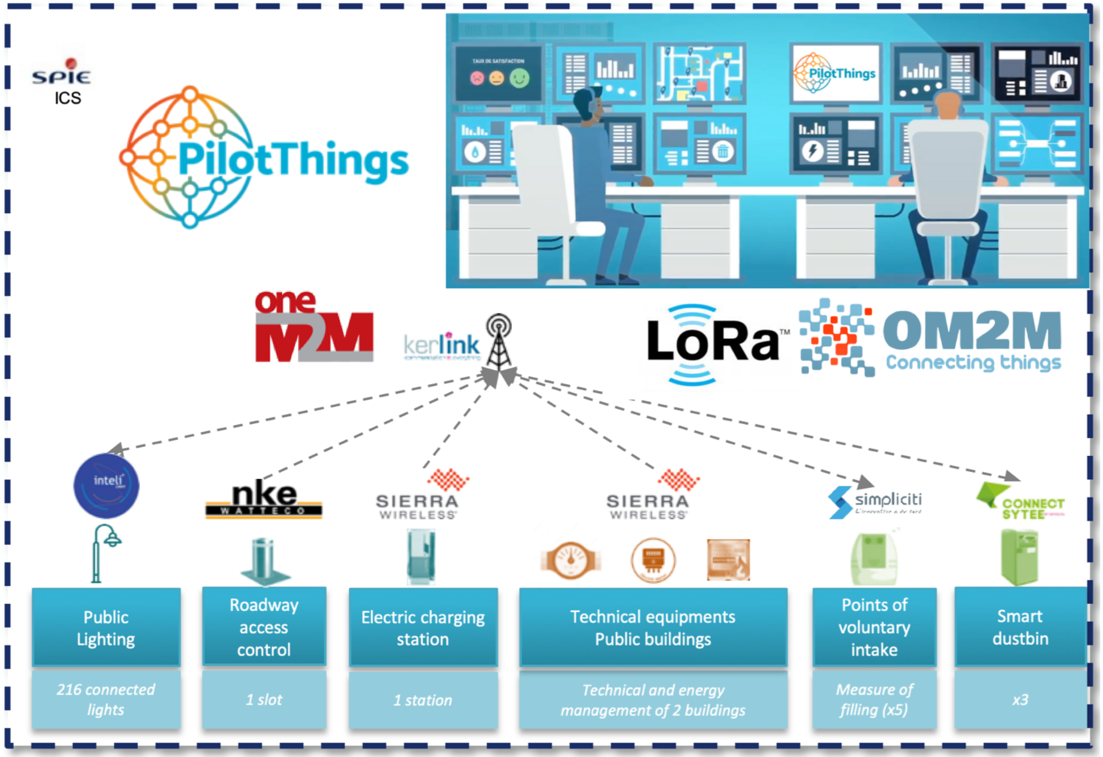
Example: City of Bordeaux

- Save energy and maintenance cost of public lighting
- Manage data and equipments: building, smart meters, Electric charging stations, street access, waste collect, ….

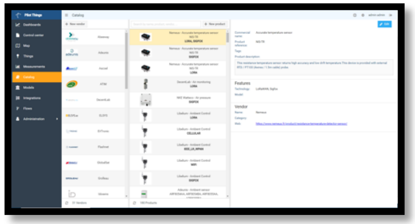

Create a multi channel IoT network

Locate objects

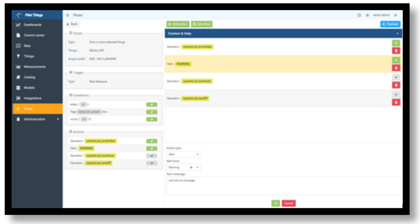

Manage connected things



Public Lighting	Roadway access control	Electric charging station	Technical equipments Public buildings	Points of voluntary intake	Smart dustbin
216 connected lights	*1 slot*	*1 station*	*Technical and energy management of 2 buildings*	*Measure of filling (x5)*	*x3*


Things as a Service - TaaS

Supervision


Automation of operations

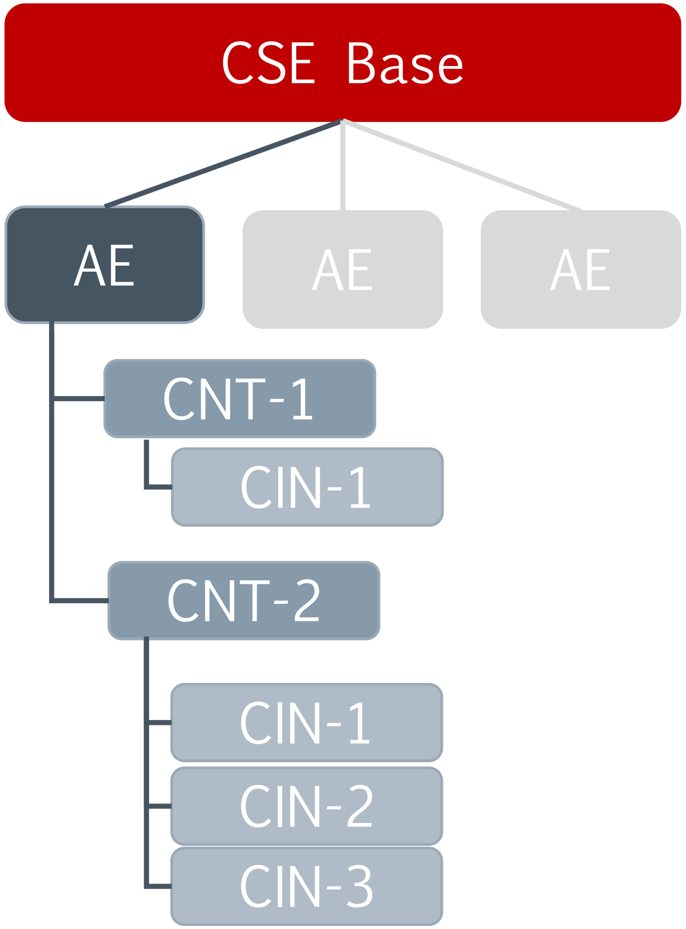
PilotThings Connect your world

Standardized API

- Based on REST architecture **(representational state transfer)**
- **Resource** oriented
  - Stored on a server
- Access using an **URI**
  - http://www.example.com/wiki/rest
  - http://www.example.com/software/releases/latest.tar.gz
- **Representation** of resources
  - Used in exchange with client/user
  - Can be any representation format: XML, JSON, BSON, …
- **Link** to other resources
  - Dependencies, hierarchy is represented by link in resource representation

The basic resources

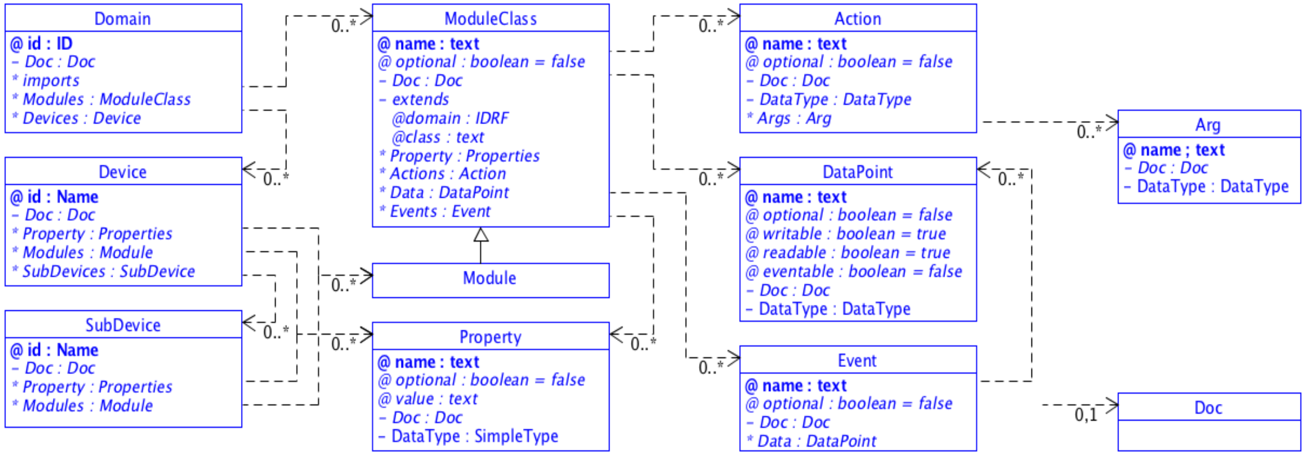
- Common Service Entity *(CSE)*
- Container *(CNT)*
- Application Entity *(AE)*
- Container *(CNT)*
- Content Instance *(CIN)*
- ….



1. Onem2m.org, TS-0001 Functional Architecture

Information model - SDT

- Provide an harmonized abstract information model
- Based on SDT (Smart Device Template)
- Document: SDT based Information Model and Mapping for Vertical Industries (TS-0023-V4.1.0)
- Design : structure / set of rules (naming, stateless, domain, …)
- Abstraction, flexibility (inheriance, extensibility, modularization), XML encoding
- Data structure composed of **Device** objects, made of optional or mandatory functional units (**Modules**) that are composed of readable and/or writable **data points**.



Domain
@ id : ID
– Doc : Doc
** imports*
** Modules : ModuleClass*
** Devices : Device*

Device
@ id : Name
– Doc : Doc
** Property : Properties*
** Modules : Module*
** SubDevices : SubDevice*

SubDevice
@ id : Name
– Doc : Doc
** Property : Properties*
** Modules : Module*

ModuleClass
@ name : text
@ optional : boolean = false
– Doc : Doc
– extends
@domain : IDRF
@class : text
** Property : Properties*
** Actions : Action*
** Data : DataPoint*
** Events : Event*

Module

Property
@ name : text
@ optional : boolean = false
@ value : text
– Doc : Doc
– DataType : SimpleType

Action
@ name : text
@ optional : boolean = false
– Doc : Doc
– DataType : DataType
** Args : Arg*

DataPoint
@ name : text
@ optional : boolean = false
@ writable : boolean = true
@ readable : boolean = true
@ eventable : boolean = false
– Doc : Doc
– DataType : DataType

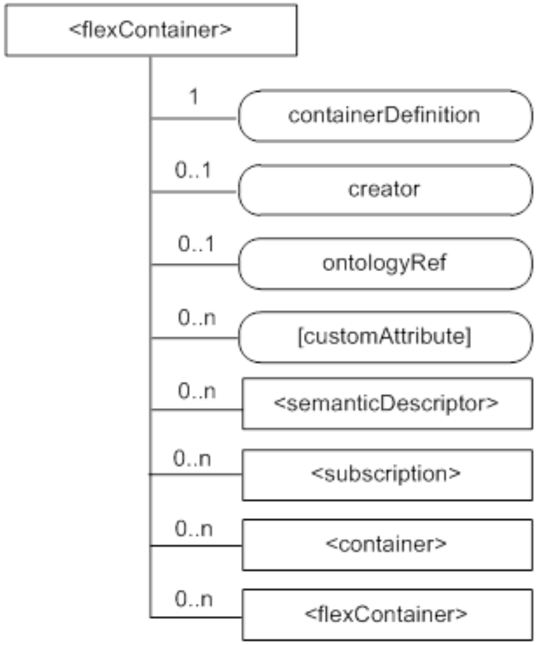
Event
@ name : text
@ optional : boolean = false
– Doc : Doc
** Data : DataPoint*

Arg
@ name ; text
– Doc : Doc
– DataType : DataType

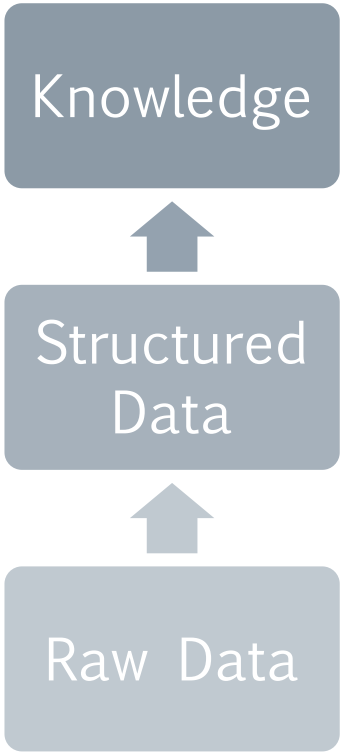
Doc

Information model - SDT

- Exemple: Domain (org.onem2m.home), Device (DeviceLight), ModuleClass (binarySwitch)
- Around 100 Module classes (3Dprinter, airFlow, alarmSpeaker, battery, binarySwitch, colour, ….)
- Around 60 device models in different domains (deviceAudioReceiver, deviceDoorLock, deviceSmartPlug, deviceStreetLightController, …)
- Used flexContainer resource in oneM2M



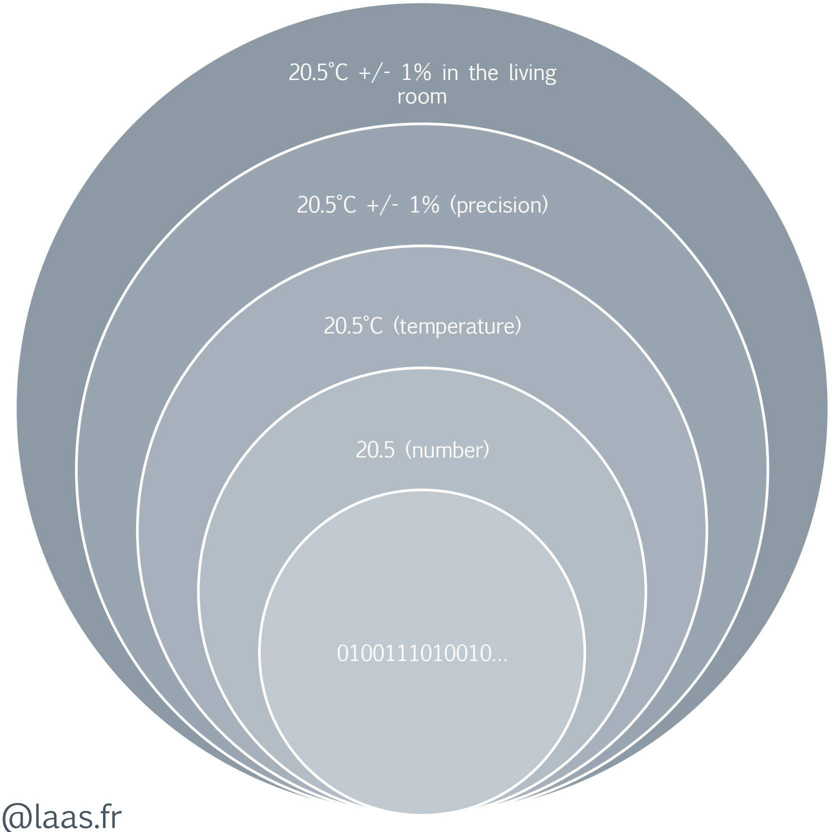
Transformation of a message into a more expressive format



Knowledge

Structured Data

Raw Data



20.5°C +/- 1% in the living room

20.5°C +/- 1% (precision)

20.5°C (temperature)

20.5 (number)

0100111010010...

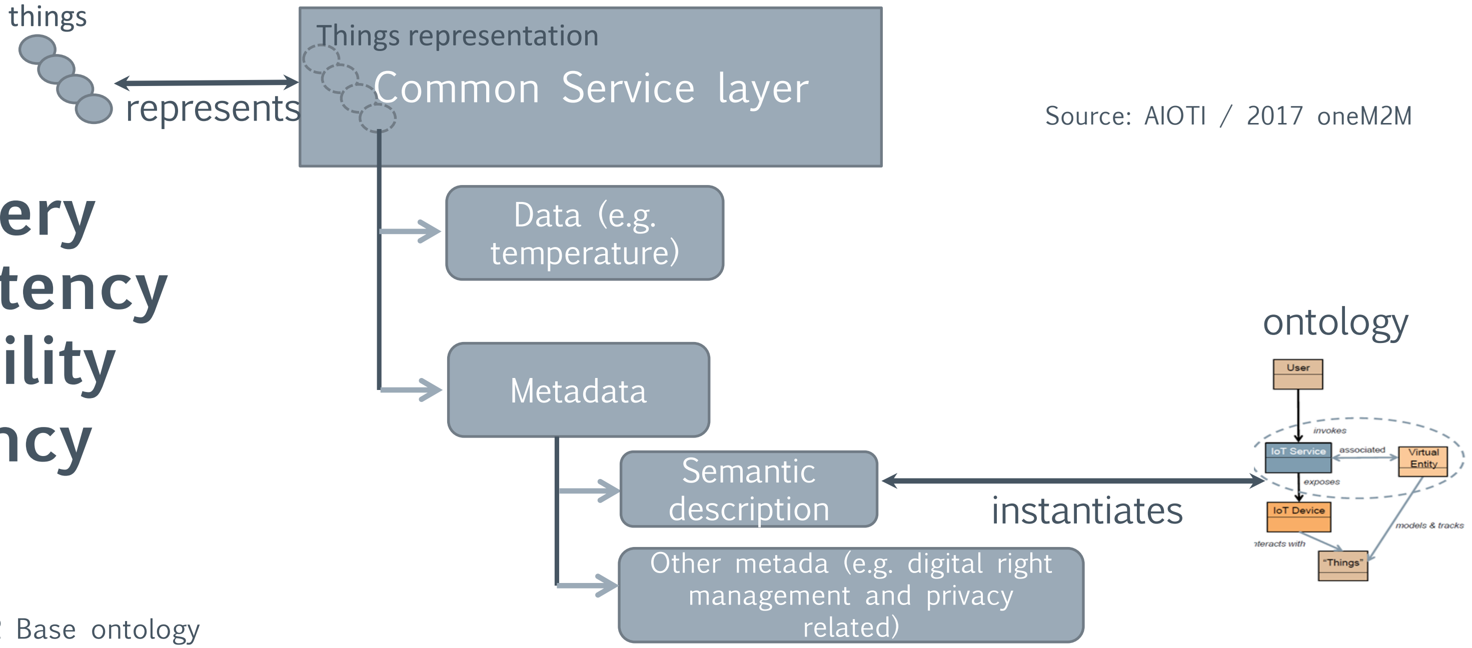
Semantic Functionalities under standardization by oneM2M

- ▸ Need for semantic
  - Semantic enables Applications to directly interact with real-world entities, through their virtual annotated representation
  - Semantic support for interworking between various applications (TS-0030-Ontology based Interworking)
- ▸ Functionalities
  - ○ Semantic Queries (e.g. Discovery)
  - ○ Support for Data Analytics
  - ○ Support for Semantic Mash-ups
- ▸ Required Foundations
  - ○ Semantic Annotation
  - ○ **Ontology**
  - ○ Semantic Reasoning

1. Onem2m.org, TS-0012 Base ontology

Semantic and ontology

- ▸ An ontology is a formal and explicit specification of a shared conceptualisation [Studer, 1998]
- **Concepts** : Sensors, Measure, Temperature…
- **Relations** : A watchs B, C characterizes D…
- **Axioms** : Every Sensors that makes a measure of Temperature is a SensorOfTemperature



things

represents

Things representation

Common Service layer

Data (e.g. temperature)

Metadata

Semantic description

Other metada (e.g. digital right management and privacy related)

instantiates

ontology

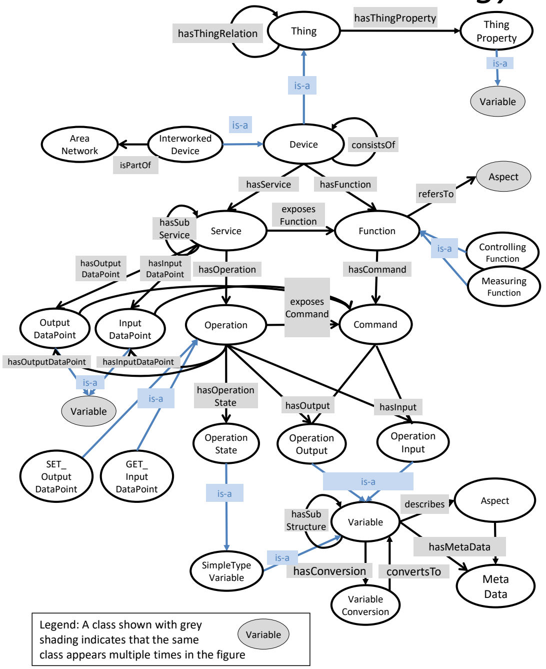
Source: AIOTI / 2017 oneM2M

=>Discovery
=>Consistency
=>Scalability
=>Efficiency

1. Onem2m.org, TS-0012 Base ontology

Work on Semantics – the oneM2M ontology

The oneM2M Base Ontology



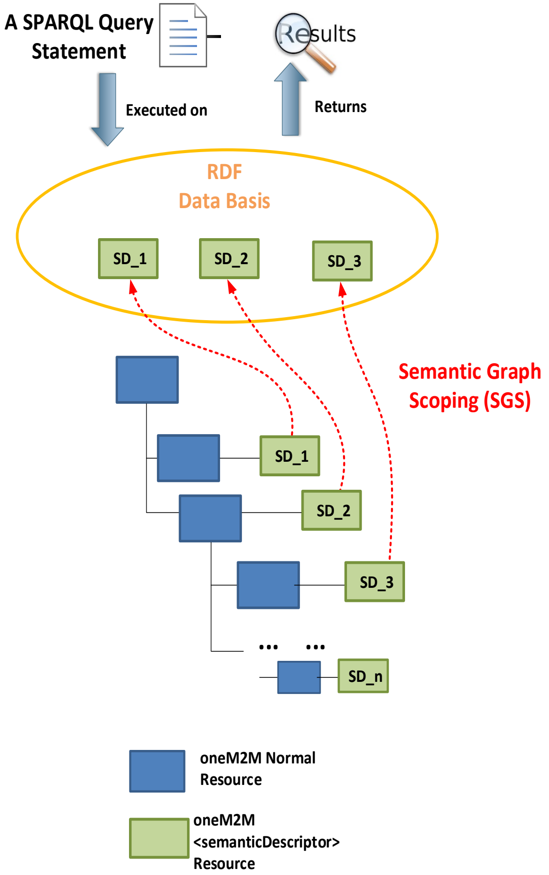
- oneM2M allows to ***annotate*** application specific resources (M2M data) with semantic description.
  - Uses a specialized resource type *<semanticDescriptor>*
  - Can contain proprietary semantics

  or

  - Semantics according to a published ontology
- The oneM2M ***base ontology*** is a top-level ontology that allows to create sub-classes (or equivalence classes) for application-level ontologies
  - Example: Smart Appliances Reference Ontology (SAREF)
- Ontologies can be used in oneM2M to describe the application specific data model of an external system for the purpose of interworking.
  - oneM2M ***Generic Interworking*** uses such an ontology to enable interworking of oneM2M entities with devices of the external system

Work on Semantics – Semantic Query

- oneM2M includes a semantic query feature that includes both discovery and query capabilities
  - Semantic resource discovery is used to discover resources: Give me the resources that represent the temperature sensors located in Room 1.
  - Semantic query is used to extract "useful knowledge" (to answer the query) over a set of "RDF data basis". What is the manufacture name and production year of the temperature sensors located in Room 1?
- To successfully execute a semantic query requires appropriate semantic graph scoping and extra information represented in RDF triples
  - Semantic Graph Scoping: How to collect RDF triples from semantic descriptors (distributed in the resource tree) to construct a RDF data basis for a given semantic query.
  - Representing Extra Information in RDF Triples: This is for how to query information that was originally not stored as RDF triples, such as data stored in <*contentInstance*> resource (or other oneM2M attributes such as *expirationTime*, etc.).



Semantic in oneM2M

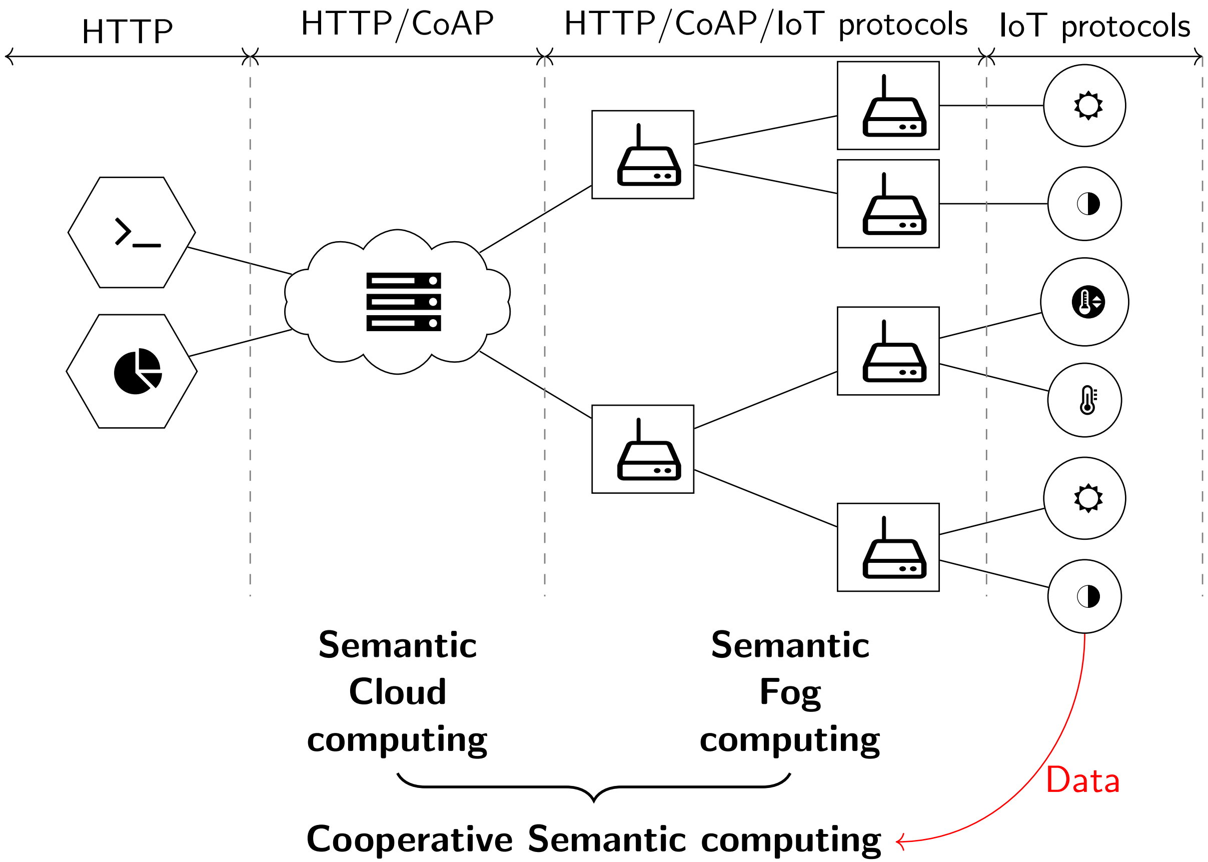
- Resources (TS-0034)
  - semanticDescriptor: store a semantic description of a resource
  - semanticFanOutPoint: a virtual resource for semantic discovery or query
  - Resources for mashup operation, ontology repository, queries, validation, Acces Control Ontology
- Use of any ontologies: SSN, SAREF, IoT-O
- Work need to be continued on data analytics, reasoning or scalability

From the IoT to the SWoT (Semantic Web of Things)

- IoT
  - Mutliple applications domains
  - Hardware, communication and software heterogeneity
- IoT constraints
  - Memory, processing power and energy limitations
  - Dynamic network topology

- Semantic Web
  - Native human and machine understandability
  - Interoperability based on shared conceptualizations
- Semantic Web requirements
  - Resource-consuming processing and formats
  - Limited scalability

SWoT architecture with oneM2M

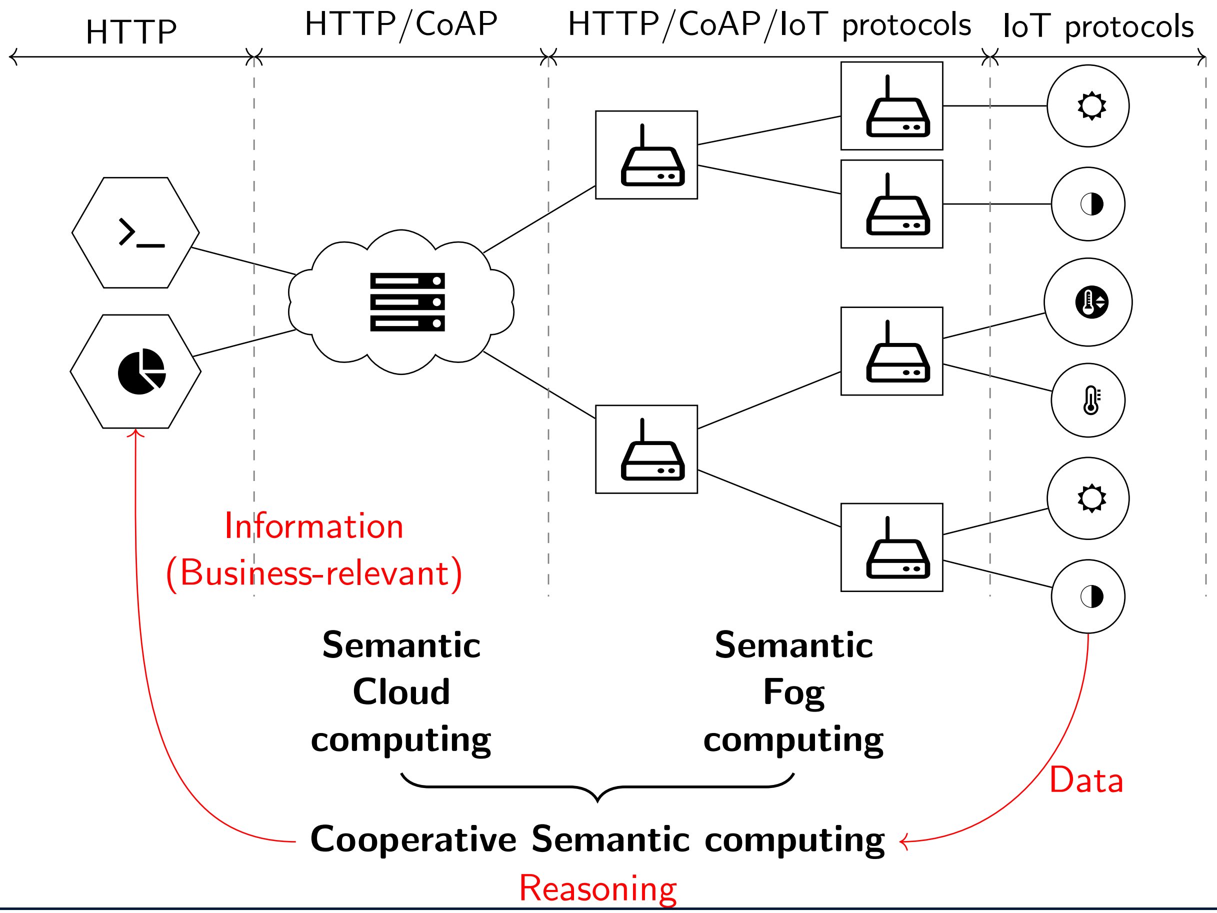


Semantic Cloud computing

Semantic Fog computing

Cooperative Semantic computing

SWoT architecture for Industry

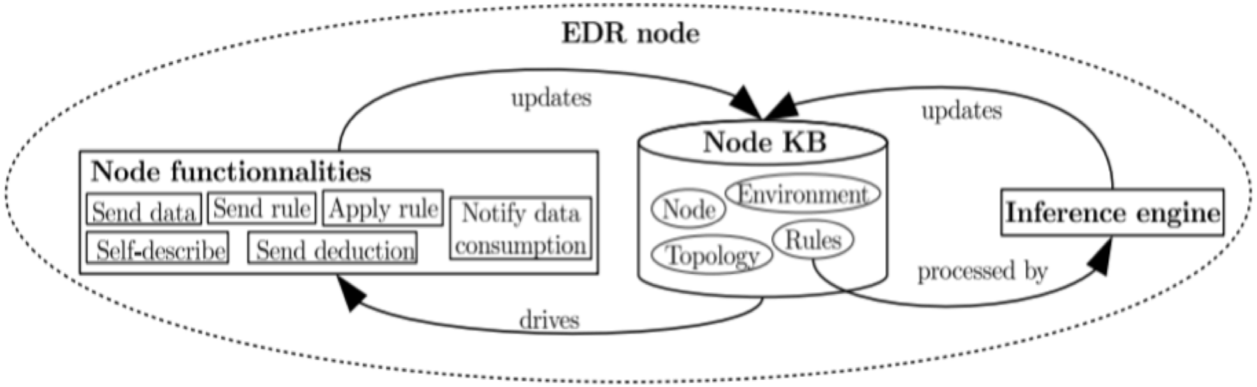


In 2025, 75% of data collected will be analysed outside of the cloud[1]

[1] https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and- operations-leaders/

Emergent Distributed Reasoning – EDR[1]

- A generic approach to dynamic distribution of rule-based reasoning
- Associated to a propagation algorithm
- Strategy-agnostic
- A new IPE

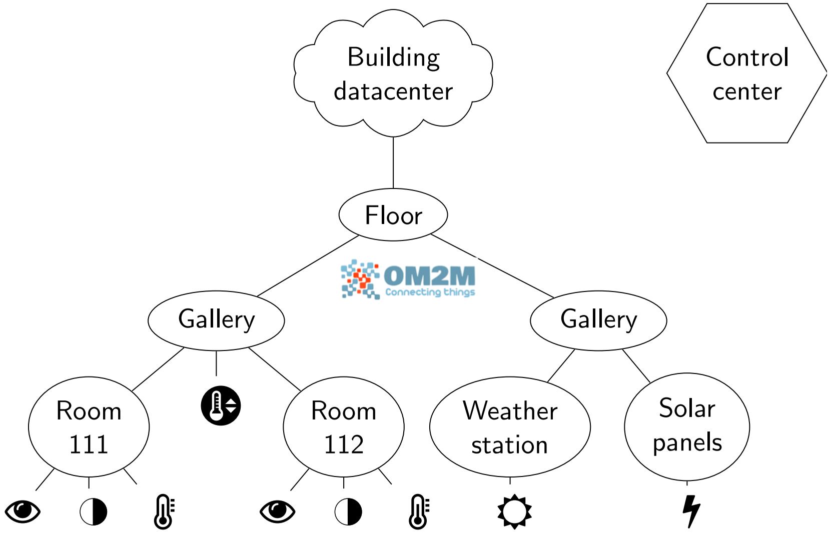


- Specialisation: EDRτ
  - Strategy: propagates rules as close to sensors as possible

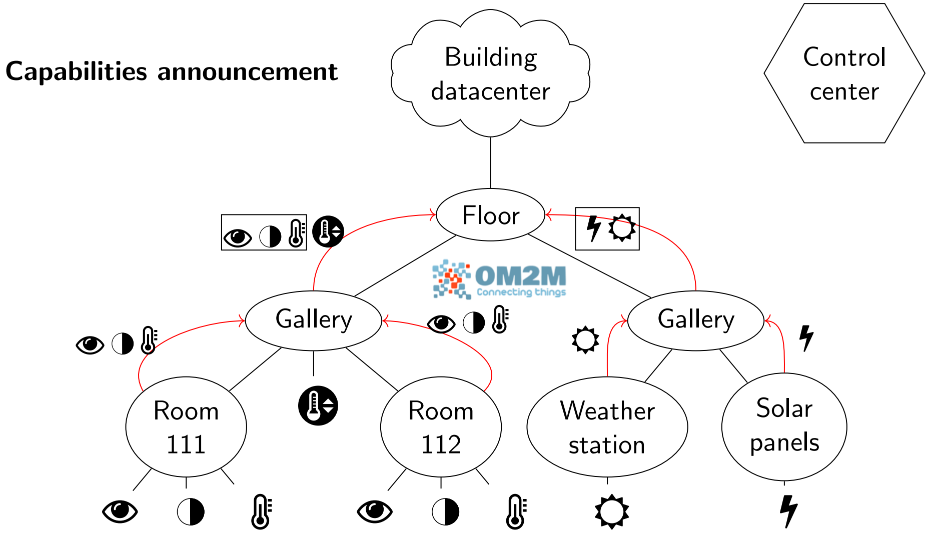
[1] N. Seydoux, K. Drira, N. Hernandez, T. Monteil Towards Cooperative Semantic Compu- ting : a Distributed Reasoning approach for Fog-enabled SWoT. In Proceedings of the 26th International Conference on Coope- rative Information Systems (CoopIS), October 2018.

EDRτ : announcement

EDR$_{\mathcal{T}}$ by the example

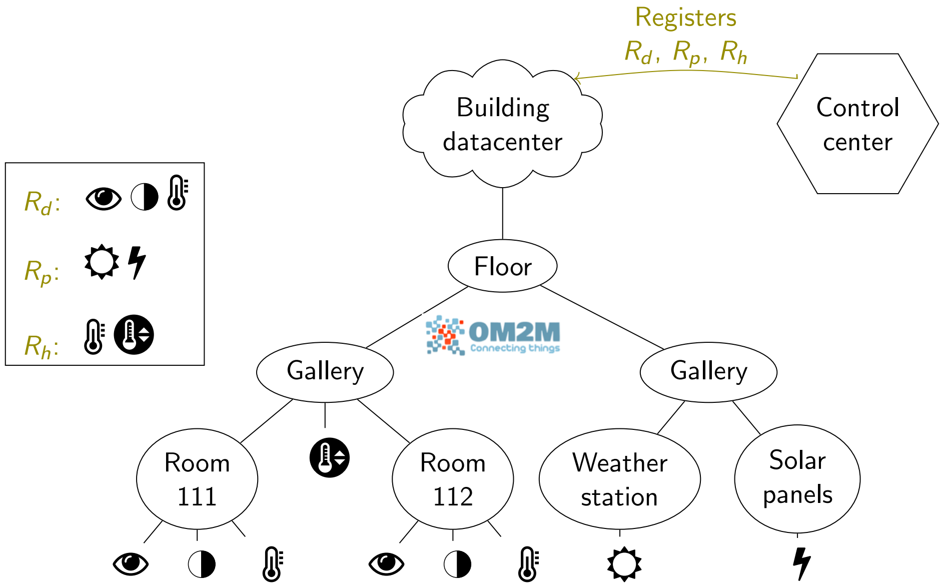


EDR$_{\mathcal{T}}$ by the example

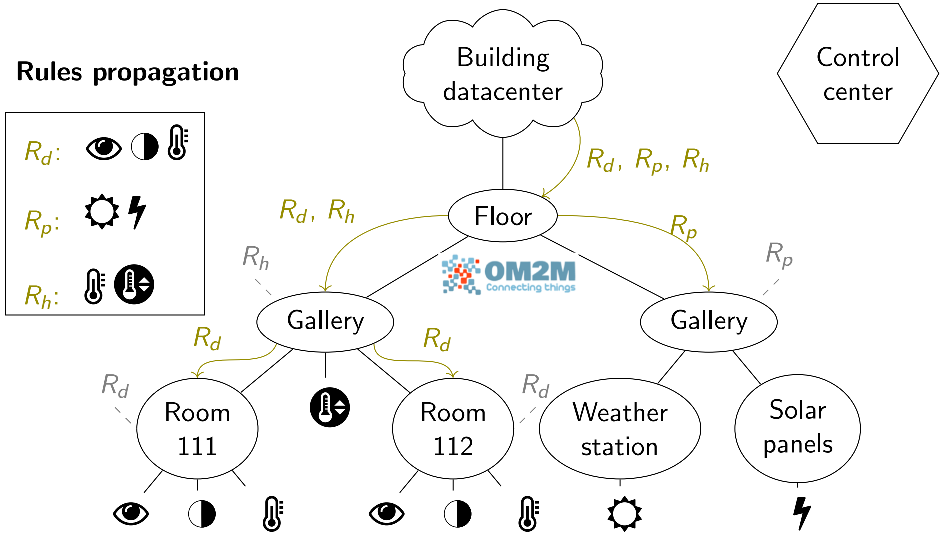


EDRτ : rules propagation

EDR$_\mathcal{T}$ by the example



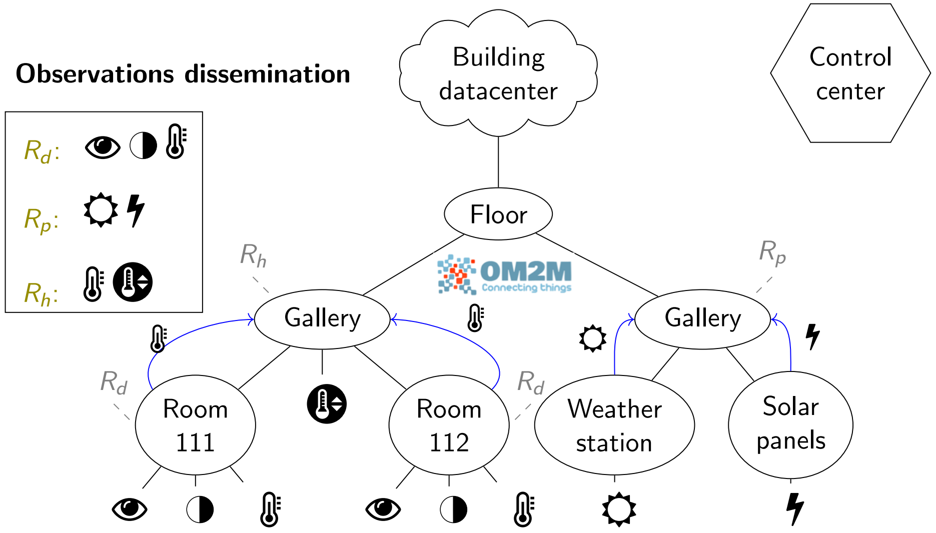
EDR$_\mathcal{T}$ by the example



Research activities

EDRτ : data and rules dissemination

EDR$_{\mathcal{T}}$ by the example



- Scalability
- Autonomous systems
- Flexibility to specialise EDR

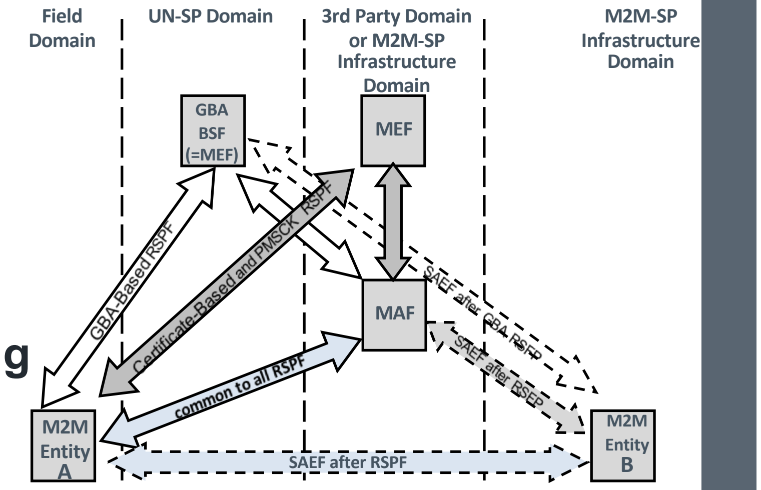
Security in an IoT architecture: hard challenges

- 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

Security in oneM2M

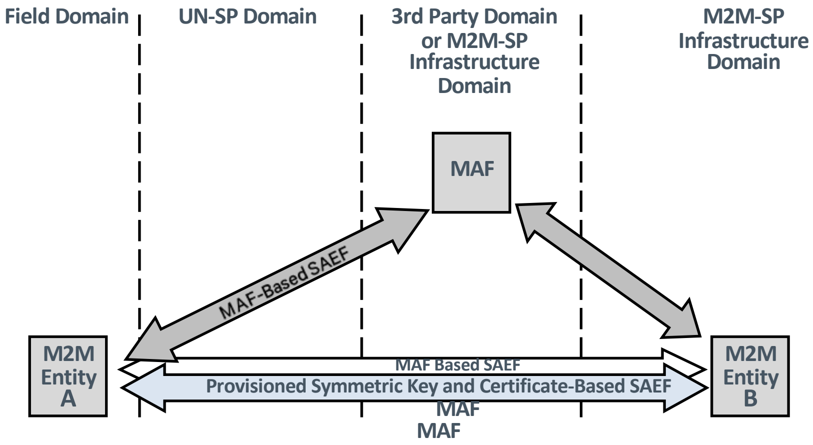
- Some documents: TS-0003 Security Solutions, TS-0022 Field Device Configuration, TS-0032 MAF and MEF Interface Specification, …
- Definition of Security Functions Layers:
  - Identification, Authentication, Authorization, Security Association, Sensitive Data Handling and Security Administration
- Enrolment service
  - provisioning and configuration phases
  - Remote Security Provisioning Frameworks (RSPF) :
    - **Pre-Provisioned Symmetric Enrolee Key / Certificate-Based Remote Security Provisioning Framework / Generic Bootstrapping Architecture**
    - **Based on M2M Enrolment Function (MEF) that use M2M authentication Function (MAF)**

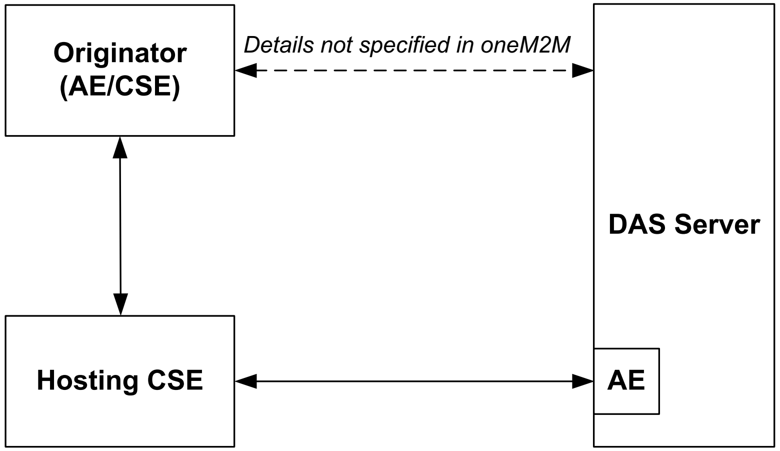


Source: oneM2M TS-0003

Security in oneM2M

- Authentification
  - **Provisioned Symmetric Key / Certificate-Based Security Association / M2M Authentication Function (MAF)**
- Secure communications
  - HTTPS, CoAP DTLS
- Authorization
  - Based on Access Control Policy
  - Could have dynamic authorization with DAS (Dynamic Authorisation Server)


Field Domain
UN-SP Domain
3rd Party Domain or M2M-SP Infrastructure Domain
M2M-SP Infrastructure Domain
MAF
MAF-Based SAEF
M2M Entity A
M2M Entity B
MAF Based SAEF
Provisioned Symmetric Key and Certificate-Based SAEF
MAF
MAF

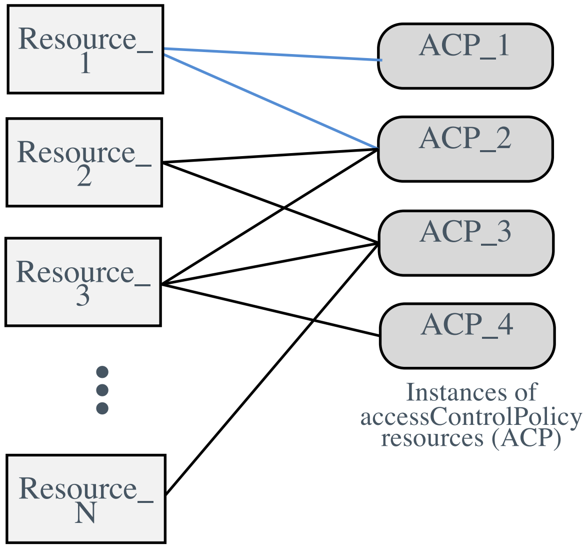


Source: oneM2M TS-0003

Thierry Monteil – monteil@laas.fr

Access control description

The resource **Access Control Policy** *(ACP)*



Source: oneM2M TS-0003

```
<m2m:acp xmlns:m2m="…" rn="">
   <pv>
       <acr>
           <acor></acor>
           <acop></acop>
       </acr>
   </pv>
   <pvs>
       <acr>
           <acor></acor>
           <acop></acop>
       </acr>
   </pvs>
</m2m:acp>
```

Privileges:
Manage the right for resources of this ACP

Self-privileges:
Manage the right to access or modify this resource

Acces control description

The resource **Access Control Policy** *(ACP)*

```
<m2m:acp xmlns:m2m="…" rn="">
  <pv>
     <acr>
        <acor></acor>
        <acop></acop>
     </acr>
  </pv>
  <pvs>
     <acr>
        <acor></acor>
        <acop></acop>
     </acr>
  </pvs>
</m2m:acp>
```

Signification

acr = « Access Control *Rule* »

acor = « Access Control *Originators* »

acop = « Access Control *Operations* »

Opération	Code
CREATE	1
RETRIEVE	2
UPDATE	4
DELETE	8
NOTIFY	16
DISCOVERY	32

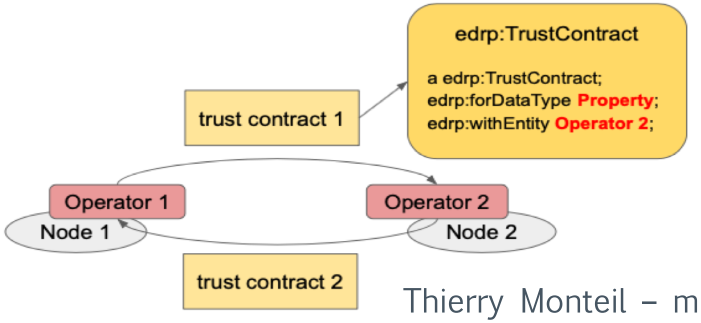
Example:

```
<acr>
   <acor>admin</acor>
   <acop>63</acop>
</acr>
<acr>
   <acor>guest arthur</acor>
   <acop>34</acop>
</acr>
```

Research activities

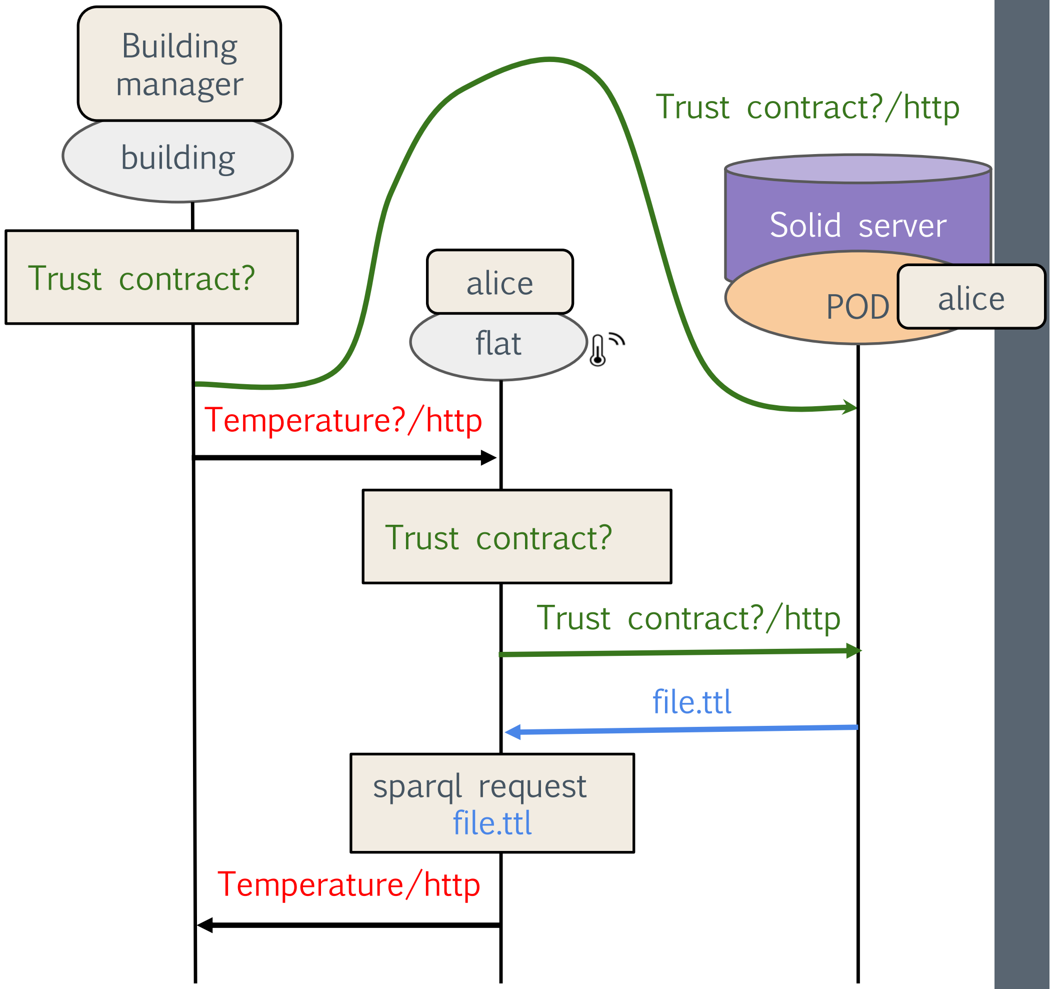
EDR the return

- Emergent Distributed Reasoning with privacy - EDRp
  - Use of POD (Personal Online Data Store) / SOLID servers (inrupt.com)
    - Each user define his own strategy
  - Definition of operator of IoT nodes
  - Definition of Trust contracts



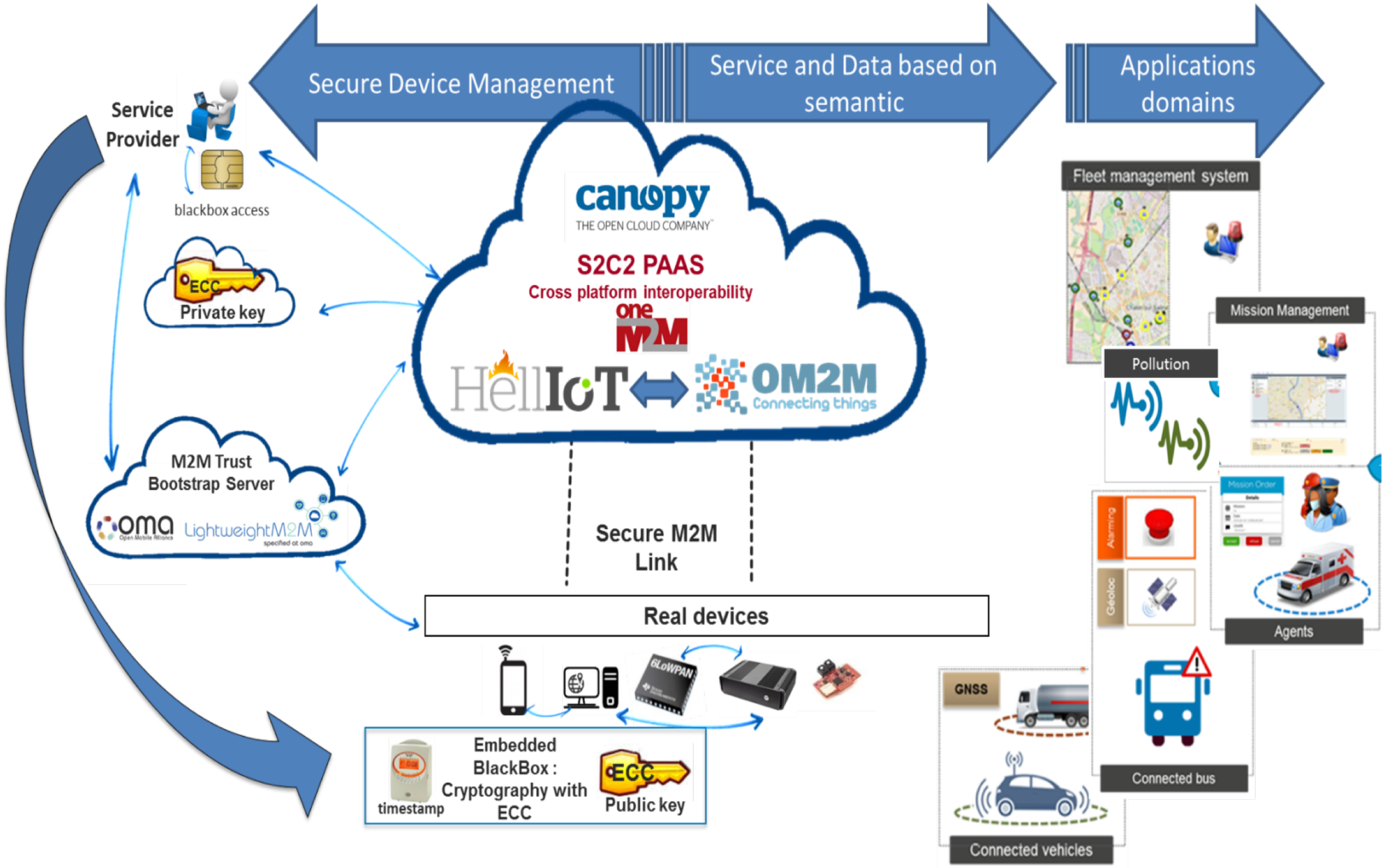
edrp:TrustContract

```
a edrp:TrustContract;
edrp:forDataType Property;
edrp:withEntity Operator 2;
```



Testbed

S2C2 - Smart Services for Connected vehiCles



S2C2

Atos

e-device TECHNOLOGY Connecting Devices

LAAS CNRS

m3 SYSTEMS

Thierry Monteil – monteil@laas.fr

Keep in mind

- oneM2M
  - Made by standard organization with several hundred companies
  - IoT services platform
  - Interoperability by design
  - Define:
    - Architecture
    - Common services functions
    - Information model
  - Release 3
- Push research results / innovation
  - Quality of service
  - Distributed dynamic management of IoT architecture (service, data, network, …)
  - Autonomous systems => fog computing architecture
  - Data usage

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

TOULOUSE

« The Pink City » due to the color of its walls

Industry, Culture, Education and Research

- Created in 120 B.C.
- 1st Region in R&D investment: 4.8% of Gross Domestic Product
- Major aeronautics and aerospace Companies: Airbus Group…
- The 2nd university city in France with 120,000 students
- Dynamic region with fast growth, creating jobs !
- Own culture: popular sports, events, traditional food…

© Cité de l'Espace

© Airbus

© Ville de

INSA TOULOUSE

LAAS CNRS

©CNRS Photothèque – FRESILLON Cyril

Thank you

- **Thierry Monteil** – monteil@laas.fr (Professor at INSA – Univ. of Toulouse / Researcher at LAAS-CNRS)