Supporting Internet of Things Activities on Innovation Ecosystems

H2020 – UNIFY-IoT Project

Deliverable 05.02

Interoperable IoT Platforms

Standards Framework

Revision : 1.00
Due date : 28-02-2018
Actual submission date : 23-03-2018

Lead partner : ETSI

<table>
<thead>
<tr>
<th>Dissemination level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PU</td>
<td>Public</td>
</tr>
<tr>
<td>PP</td>
<td>Restricted to other programme participants (including the Commission Services)</td>
</tr>
<tr>
<td>RE</td>
<td>Restricted to a group specified by the consortium (including the Commission Services)</td>
</tr>
<tr>
<td>CO</td>
<td>Confidential, only for members of the consortium (including the Commission Services)</td>
</tr>
</tbody>
</table>

X
## Summary

<table>
<thead>
<tr>
<th>No and name</th>
<th>D05.02 Interoperable IoT Platforms Standards Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
<td>Released</td>
</tr>
<tr>
<td><strong>Due</strong></td>
<td>m20</td>
</tr>
<tr>
<td><strong>Date</strong></td>
<td>28-02-2018</td>
</tr>
<tr>
<td><strong>Author(s)</strong></td>
<td>Philippe Moretto (ETSI STF – Special Task Force)</td>
</tr>
<tr>
<td><strong>Editor</strong></td>
<td>Patrick Guillemin (ETSI), Ovidiu Vermesan (SINTEF)</td>
</tr>
<tr>
<td><strong>DoW</strong></td>
<td>Provide a report describing the interoperable IoT platforms standards framework that was developed with the stakeholders of AIOTI and based on the cooperation work in AIOTI WG03</td>
</tr>
</tbody>
</table>

### Comments

<table>
<thead>
<tr>
<th>V</th>
<th>Date</th>
<th>Author</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.01</td>
<td>14-08-2017</td>
<td>ETSI</td>
<td>Advanced draft</td>
</tr>
<tr>
<td>0.02</td>
<td>04-09-2017</td>
<td>SINTEF</td>
<td>Structured draft.</td>
</tr>
<tr>
<td>0.1</td>
<td>25-09-2017</td>
<td>ETSI</td>
<td>Initial content included, no edition.</td>
</tr>
<tr>
<td>0.2</td>
<td>14-01-2018</td>
<td>ETSI</td>
<td>Proposed new ToC and content for Jan. 15th meeting.</td>
</tr>
<tr>
<td>0.3</td>
<td>23-01-2018</td>
<td>ETSI</td>
<td>New draft based on available material and new ToC</td>
</tr>
<tr>
<td>0.41</td>
<td>14-03-2018</td>
<td>ETSI</td>
<td>New version with SAREF inputs</td>
</tr>
<tr>
<td>0.50</td>
<td>16-03-2018</td>
<td>ETSI</td>
<td>Editor review</td>
</tr>
<tr>
<td>0.51</td>
<td>17-03-2018</td>
<td>ETSI</td>
<td>Editor review</td>
</tr>
<tr>
<td>0.52</td>
<td>21-03-2018</td>
<td>ETSI</td>
<td>Final review</td>
</tr>
<tr>
<td>1.0</td>
<td>23-03-2018</td>
<td>SINTEF</td>
<td>Final review. Release</td>
</tr>
</tbody>
</table>

### Disclaimer

The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

The document reflects only the author’s views and the EC is not liable for any use that may be made of the information contained therein.
Table of contents

1. Executive summary ............................................................................................................. 8
2. Introduction .......................................................................................................................... 9
   2.1 Purpose and target group of this deliverable ..................................................................... 9
   2.1.1 Scope and purpose of this document ......................................................................... 9
   2.1.2 Target group for this document ................................................................................ 9
   2.2 Contributions of partners .............................................................................................. 9
3. A Reference Framework for IoT Standards ....................................................................... 10
   3.1 Introduction ................................................................................................................... 10
   3.2 The AIOTI Reference Framework ................................................................................. 10
      3.2.1 Horizontal and Vertical Mappings ........................................................................ 10
      3.2.2 High-Level Architecture (HLA) ........................................................................... 10
      3.2.3 An evolving framework ....................................................................................... 11
   3.3 Interoperability: stack and patterns .............................................................................. 11
      3.3.1 Interoperability: horizontal and vertical aspects .................................................. 11
      3.3.2 The Interoperability stacks ................................................................................... 12
      3.3.3 IoT-EPI White Paper patterns of IoT interoperability .......................................... 13
   3.4 High-Level (Reference) Architecture ............................................................................ 14
   3.5 Specific aspects .............................................................................................................. 15
      3.5.1 Semantic Interoperability .................................................................................... 15
      3.5.2 Marketplaces and APIs ....................................................................................... 19
4. The IoT Platforms and the Standards Framework ............................................................ 21
   4.1 Introduction ................................................................................................................... 21
   4.2 IoT Standards ................................................................................................................ 21
   4.3 IoT Platforms ................................................................................................................ 21
      4.3.1 Introduction ........................................................................................................... 21
      4.3.2 The platforms in the IoT-EPI Projects .................................................................. 22
      4.3.3 The platforms identified by UNIFY-IoT ............................................................... 23
      4.3.4 Other platforms ................................................................................................... 23
   4.4 Standards and support of interoperability in IoT platforms ............................................ 24
      4.4.1 Introduction ........................................................................................................... 24
      4.4.2 Examples of interoperability support in IoT-EPI projects ..................................... 24
5. ETSI SmartM2M and oneM2M ......................................................................................... 28
   5.1 Introduction ................................................................................................................... 28
   5.2 SAREF Rationale ......................................................................................................... 29
6. ETSI Smart city .................................................................................................................. 32
   6.1 Introduction ................................................................................................................... 32
   6.2 Smart City IoT interoperability ...................................................................................... 32
   6.3 Core objectives of TC SmartM2M, TC SmartBAN and ISG CIM ................................. 33
7. AIOTI WG03 cooperation on interoperable IoT Platforms .............................................. 34
   7.1 Introduction ................................................................................................................... 34
   7.2 Creation of AIOTI since 2015 ........................................................................................ 35
   7.3 AIOTI work and recommendations ............................................................................. 36
      7.3.1 AIOTI IoT Landscape ............................................................................................ 37
      7.3.2 Common IoT high level architecture (HLA) .......................................................... 37
      7.3.3 IoT Semantic Interoperability (SemIoP) ............................................................... 38
   7.4 AIOTI recommendations for EU-funded IoT projects .................................................... 38
   7.5 Summary of IoT-EPI platforms in liaison with AIOTI .................................................. 38
   7.6 AIOTI Analysis of IoT Platforms and IoT-EPI .............................................................. 40
   7.7 What’s next for AIOTI? ............................................................................................... 40
8. Challenges, Issues and Gaps ............................................................................................. 42
8.1 Impact of IoT standards on interoperability and platforms..................................................42
  8.1.1 Design and deployment of IoT Systems.................................................................42
  8.1.2 Privacy and data confidentiality ......................................................................43
  8.1.3 Security ...........................................................................................................43
  8.1.4 Regulation .........................................................................................................43
8.2 Gaps .........................................................................................................................44
8.3 Standards in support of interoperability in IoT .........................................................45

9. References ..................................................................................................................46

10. Appendices As Published by IoT EPI Task Force ......................................................47
  10.1 The IoT-EPI Platforms ..............................................................................................47
      10.1.1 Platforms in the Agile project .................................................................47
      10.1.2 Platforms in the bloTope project ............................................................47
      10.1.3 Platforms in the BIG-IoT project ............................................................48
      10.1.4 Platforms in the INTER-IoT project .........................................................49
      10.1.5 Platforms in the symbIoTe project .........................................................50
      10.1.6 Platforms in the TagItSmart project .......................................................51
      10.1.7 Platforms in the VICINITY project .........................................................51

List of figures

Figure 1: Functional Model of the AIOTI HLA ............................................................................11
Figure 2: The AIOTI Interoperability Stack ...........................................................................12
Figure 3: The AIOTI Three Layer Functional Model ..........................................................13
Figure 4: Patterns of IoT interoperability defined in “IoT Platforms Interoperability Approaches
White Paper 2018” .................................................................................................................13
Figure 5: A Virtualised IoT High-Level Architecture ..........................................................14
Figure 6: The Three IoT Software Stacks ..............................................................................15
Figure 7: Semantic interoperability functional layers ...........................................................16
Figure 8: Applicability of semantic technologies to IoT HLA layers ....................................17
Figure 9: UNIFY-IoT: Leading IoT Platforms selected for in-depth analysis ....................23
Figure 10: List of 13 Working Groups of AIOTI ................................................................36

List of tables

Table 1: Platforms used by the IoT EPI Projects ..................................................................23
Table 2: Telecommunications Originated Platforms .........................................................23
Table 3: Perceived criticality of some Standards Gaps (Source: CREATE-IoT) .................44
Table 4: AGILE platforms ..................................................................................................47
Table 5: BloTope platforms .................................................................................................48
Table 6: BIG IoT platforms ................................................................................................49
Table 7: Inter IoT platforms .................................................................................................50
Table 8: symbIoTe platforms ..............................................................................................51
Table 9: TagItSmart platforms ...........................................................................................51
Table 10: Vicinity platforms ...............................................................................................52
# List of acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3GPP</td>
<td>3rd Generation Partnership Project, <a href="http://www.3gpp.org">www.3gpp.org</a></td>
</tr>
<tr>
<td>4G</td>
<td>see LTE (3GPP)</td>
</tr>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>AIOTI</td>
<td>Alliance for Internet of Things Innovation <a href="http://www.aioti.eu">www.aioti.eu</a></td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>ARIB</td>
<td>Association of Radio Industries and Businesses, Japan</td>
</tr>
<tr>
<td>ATIS</td>
<td>Alliance for Telecommunications Industry Solutions, US</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>CCSA</td>
<td>Communications Standards Association, China</td>
</tr>
<tr>
<td>CSP</td>
<td>Cloud Service Provider</td>
</tr>
<tr>
<td>CEN</td>
<td>European Committee for Standardization. Partner type 2 of oneM2M, <a href="http://www.cen.eu">www.cen.eu</a></td>
</tr>
<tr>
<td>CENELEC</td>
<td>European Committee for Electrotechnical Standardization. Partner type 2 of oneM2M, <a href="http://www.cenelec.eu">www.cenelec.eu</a></td>
</tr>
<tr>
<td>CIM</td>
<td>Core Information Model (in BIG IoT)</td>
</tr>
<tr>
<td>CIM</td>
<td>cross cutting Context Information Management (in ETSI ISG CIM)</td>
</tr>
<tr>
<td>CIM</td>
<td>Common Information Model (in IEC)</td>
</tr>
<tr>
<td>CREATE-IoT</td>
<td>CRoss fErtilisation through AlignmenT, synchronisation and Exchanges for IoT</td>
</tr>
<tr>
<td>EC DG CNECT</td>
<td>DG for Communications Networks, Content and Technology</td>
</tr>
<tr>
<td>EC DG GROWTH</td>
<td>DG Growth Internal Market, Industry, Entrepreneurship and SMEs</td>
</tr>
<tr>
<td>EP</td>
<td>ETSI Project</td>
</tr>
<tr>
<td>EPP</td>
<td>ETSI Partnership Project (e.g. 3GPP, oneM2M)</td>
</tr>
<tr>
<td>ETP</td>
<td>European Technology Platform</td>
</tr>
<tr>
<td>ETSI</td>
<td>European Telecommunications Standards Institute, <a href="http://www.etsi.org">www.etsi.org</a>. Partner of 3GPP and oneM2M</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>GS</td>
<td>Group Specification (in ETSI ISGs)</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile Communications</td>
</tr>
<tr>
<td>GWAC</td>
<td>Gridwise Architecture Council</td>
</tr>
<tr>
<td>HLA</td>
<td>High-Level Architecture</td>
</tr>
<tr>
<td>HMI</td>
<td>Human Machine Interface</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communications Technology</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission <a href="http://www.iec.ch">www.iec.ch</a></td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers <a href="http://www.ieee.org">www.ieee.org</a></td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>IERC</td>
<td>EC supported IoT European Research Cluster</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IIC</td>
<td>Industrial Internet Consortium</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IoT LSPs</td>
<td>IoT Large Scale Pilots, european-iot-pilots.eu</td>
</tr>
<tr>
<td>IoT-EPI</td>
<td>IoT European Platform Initiative</td>
</tr>
<tr>
<td>IPE</td>
<td>Interworking Proxy Application Entity (in oneM2M)</td>
</tr>
<tr>
<td>ISG</td>
<td>Industry Specification Group (in ETSI)</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>ISO / IEC JTC1</td>
<td>joint technical committee of the ISO and IEC</td>
</tr>
<tr>
<td>LSP</td>
<td>Large-Scale Pilots</td>
</tr>
<tr>
<td>LTE</td>
<td>3GPP/Long Term Evolution called 4G. LTE Advanced and LTE Advanced Pro are included in 4G</td>
</tr>
<tr>
<td>LTE-M</td>
<td>Long Term Evolution for Machines</td>
</tr>
<tr>
<td>Mca</td>
<td>oneM2M interface (Application Entity – Common Service Entity), <a href="http://www.onem2m.org">www.onem2m.org</a></td>
</tr>
<tr>
<td>MNC</td>
<td>Multi National Corporations</td>
</tr>
<tr>
<td>NB IoT</td>
<td>3GPP/NarrowBand IoT</td>
</tr>
<tr>
<td>O-DF</td>
<td>Open Data Format</td>
</tr>
<tr>
<td>O-MI</td>
<td>Open Messaging Interface</td>
</tr>
<tr>
<td>oneM2M</td>
<td>ETSI Partnership project Machine-to-Machine/IoT, <a href="http://www.onem2m.org">www.onem2m.org</a></td>
</tr>
<tr>
<td>OPC-UA</td>
<td>OPC is formally known as Object Linking and Embedding for Process Control, OPC-UA is OPC Unified Architecture, IEC 62541 is a standard for OPC Unified Architecture</td>
</tr>
<tr>
<td>OpenIoT</td>
<td><a href="http://www.openiot.eu/">http://www.openiot.eu/</a></td>
</tr>
<tr>
<td>OSS</td>
<td>Open Source Software</td>
</tr>
<tr>
<td>OWL</td>
<td>Ontology Web Language</td>
</tr>
<tr>
<td>QKD</td>
<td>Quantum Key Distribution (an ISG in ETSI)</td>
</tr>
<tr>
<td>QLM</td>
<td>Quantum Learning Machine</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>QSC</td>
<td>Quantum Safe Cryptography (a TC CYBER WG in ETSI)</td>
</tr>
<tr>
<td>RDF</td>
<td>Resource Description Framework</td>
</tr>
<tr>
<td>RIA</td>
<td>Research and Innovation Action</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>SAREF</td>
<td>Smart Appliance REFerence ontology / Smart Applicatons REFerence ontology</td>
</tr>
<tr>
<td>SDK</td>
<td>Software Development Kit</td>
</tr>
<tr>
<td>SDO</td>
<td>Standards Developing Organisation</td>
</tr>
<tr>
<td>SEAS</td>
<td>Smart Energy Aware Systems</td>
</tr>
<tr>
<td>SemIoP</td>
<td>Semantic interoperability</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreements</td>
</tr>
<tr>
<td>SmartBAN</td>
<td>Smart Body Area Networks</td>
</tr>
<tr>
<td>SoS</td>
<td>Systems-of-Systems</td>
</tr>
<tr>
<td>SSO</td>
<td>Standards Setting Organisation</td>
</tr>
<tr>
<td>STF</td>
<td>Specialist Task Force</td>
</tr>
<tr>
<td>TC</td>
<td>Technical Committee</td>
</tr>
<tr>
<td>TIA</td>
<td>Telecommunications Industry Association, US</td>
</tr>
<tr>
<td>TSDSI</td>
<td>Telecommunications Standards Development Society, India</td>
</tr>
<tr>
<td>TTA</td>
<td>Telecommunications Technology Association (TTA), Korea</td>
</tr>
<tr>
<td>TTC</td>
<td>Telecommunication Technology Committee, Japan</td>
</tr>
<tr>
<td>W3C</td>
<td>World Wide Web Consortium, <a href="http://www.w3.org">www.w3.org</a></td>
</tr>
<tr>
<td>WG</td>
<td>Working Group</td>
</tr>
<tr>
<td>WoT</td>
<td>Web of Things</td>
</tr>
</tbody>
</table>
1. EXECUTIVE SUMMARY

Publishable summary

If IoT usually only refers to the capacity of a device and the way it interacts to each other and with a gateway there are indeed more than just devices in IoT. Even with devices with high computing capacity, the information collected surpass the limits of constrained mobile or fixed devices. The support that information systems and the IoT service applications can provide for using the data collected, transform it into qualitative and useful information and actions are the main challenges for IoT platforms (including loops between the physical and virtual worlds).

The story as usual will probably end-up again with only few winners among the hundreds of existing IoT Platforms today, with the happy few having properly addressed this issue in an IoT world where “there is no silos”. In addition, there will be probably new company services and offerings emerging from the new value chains.

Since basic and network connectivity have been largely the focus of SDOs and alliances for many years and consequently strategies, standards and implementations supporting this level of interoperability are generally available, on the contrary, at the interface of technical interoperability and informational interoperability, huge efforts seem urgently required in order to fulfil this full IoT potential. Strategies for syntactic and semantic interoperability, at the interface will have a major role towards this path. Since several efforts has contributed to the development of ontology editors, tools for storing and querying for data, semantic technology still remain in the hands of few ontology specialists.

Non-publishable information

This document is public.
2. INTRODUCTION

2.1 Purpose and target group of this deliverable

2.1.1 Scope and purpose of this document

This report addresses the topic of interoperability in IoT platforms and how it is supported by standards. To this extent, it introduces a framework for IoT standards specially centred around the support for interoperability, at all layers of the IoT High-Level Architecture.

The report introduces the current standards framework (High-Level Architectures, interoperability stacks and patterns, Application Programming Interfaces (APIs), Market places, etc.). It also presents a selection of platforms, in particular those used by the IoT-EPI projects. For some of these platforms, the level of support of the standards framework is considered and some recommendations are made for the IoT experts who want to use this report in the evaluation of a potential IoT platform of choice.

Regarding the standards framework, this document is mostly gathering inputs from the Alliance for Internet of Things Innovation (AIOTI) Working Group 3 (IoT Standardisation). The selection of platforms is based on inputs from the IoT-EPI Research and projects and the UNIFY-IoT Work Package 3 (see [2]).

2.1.2 Target group for this document

The target group for this document is the community of people that have to address the design, development, implementation and validation of IoT systems, making use of one or more technical platforms to that extent, and that have to ensure that the platforms they choose and/or use are supported by standards and offer the greatest possible support of interoperability at all levels.

2.2 Contributions of partners

ETSI was the task leader, editor of the document and contributor to the document. Its contributions, concerning all sections of the document, have been based on the identification of relevant material and its presentation in order to address the most recent challenges, on the identification of IoT platforms concerned by the standards framework.

SINTEF has contributed to the liaison between the EC supported IoT European Research Cluster (IERC), AIOTI WG01 (IoT Research), the AIOTI WG03 (IoT Standardisation), the SDOs and the IoT RIAs (of IoT-EPI).
3. **A Reference Framework for IoT Standards**

### 3.1 Introduction

The Internet of Things (IoT) is a very dynamic domain with a very large number of actors (industrials, research projects, standards setting organisations (SSOs), users, etc.) and a number of parallel actions and developments. Those who want to design, develop, implement and validate IoT systems are facing a number of challenges. Amongst the most pressing challenges is interoperability: it has been addressed ever since the dawn of the Information and Communication Technology (ICT) industry, AIOTI reference starting with basic interoperability standards (in particular protocols) and maturing in order to embraces more complex issues related to the development of Information Models and the need for these models to support information exchange between independent systems. The role of standardisation in the consolidation of interoperability solution is key, both by allowing to offer concrete support for various implementations, and by ensuring that the technical landscape in not a jungle of competing solutions. The IoT community is constantly refining and expanding its technical frameworks, platforms as well as standards. The definition of a framework for IoT standards is a constantly evolving target with new challenges and new solutions emerging every day. One major effort is done within the AIOTI – in particular in AIOTI Work Group 3 on IoT Standardisation – in order to address all the new challenges and provide a consistent framework over time. This section is largely based on the work of AIOTI WG03, but also takes into account complementary activities.

### 3.2 The AIOTI Reference Framework

The AIOTI – in particular the Working Group 3 - has now published several releases of its "IoT LSP Standards Framework Concepts" report (see [4]). Though initially targeted as a set of concepts for the IoT Large-Scale Pilots (LSPs) that have started at the beginning of 2017, these framework concepts are applicable to the IoT community at large (e.g. in the Industrial IoT industry segment).

The "framework concepts" are used for providing the main elements of the AIOTI WG03 shared standardisation recommendations: the "IoT Mappings" and the High-Level Architecture (HLA).

#### 3.2.1 Horizontal and Vertical Mappings

With the Horizontal and Vertical Mappings for Standards and Open Source Software (OSS), the AIOTI has undertaken a landscaping of the IoT standards field by systematically collecting information in order to structure the field:

- By distinguishing "Horizontal" activities common to all industrial sectors and by "Vertical" activities specific to a given industrial sector;
- By identifying "Knowledge Areas" (e.g., Communication and Connectivity) with the actors
- By identifying the actors engaged in these activities, essentially of two different kinds: Standards Developing/Setting Organisations (SDOs/SSOs); and OSS communities.
- By creating maps placing the actors along the different dimensions of classification. The corresponding "maps" are now well known and provide a good support, in particular, for the analysis of the platforms available and used by the actors in the IoT community.

#### 3.2.2 High-Level Architecture (HLA)

The AIOTI HLA is a common high level IoT architecture for IoT that has been developed to be applicable to the EU IoT LSPs, in particular for further discussion between the LSPs in order to promote architectural convergence.
The AIOTI HLA is similar or can be mapped to other frameworks (who mostly contributed to AIOTI HLA definition) such as those developed by ITU-T, IEEE, ETSI, oneM2M, 3GPP, W3C or IIC. An example of such a mapping is provided in the next sub-section.

The purpose of AIOTI HLA (and of the other frameworks) is in particular to support interoperability in complex IoT systems and to provide means of identifying and defining interworking standards with reduced complexity. This framework also supports the characterization of standards gaps (see [6] for example).

The Figure 1 shows the Functional Model of the AIOTI HLA:

![Figure 1: Functional Model of the AIOTI HLA](image)

### 3.2.3 An evolving framework

The technical background of IoT is a major field of interest and a fast-growing market in the industry. This technical background is evolving very fast and the AIOTI is addressing this by constantly improving its framework. Beyond the work already done on semantic Interoperability, Security and Privacy, 5G impact on IoT or IoT Identification, recent evolutions are under development involving issues such as the support of Cloud and Edge Computing, Big Data or Network Virtualisation (in particular in the context of the HLA).

### 3.3 Interoperability: stack and patterns

#### 3.3.1 Interoperability: horizontal and vertical aspects

Defining Interoperability layers is the first (fruitful) approach to clarifying the notion. Various interoperability stacks (some are described below) have been defined and used in the industries, and in particular in the IoT community, with a particular mention for the AIOTI one.

Beyond this initial approach that focuses mostly on the horizontal aspects (interoperability between elements at the same layer), it appears useful to better characterise how the different layers are interacting from this standpoint. This is, in particular, more and more useful for the IoT platforms that can better understand the associated needs and the response they may or may not provide. To this extent, the notion of “patterns” described below in section 3.3.3 is emerging.
3.3.2 The Interoperability stacks

The AIOTI Interoperability Framework has been developed within AIOTI WG03 in 2015 and specifically refers to the 2008 Gridwise Architecture Council (GWAC) work on Interoperability that is materialised in the "GWAC Stack" (see [7]) that has been adopted by AIOTI.

The AIOTI Interoperability Framework is defining a number of layers of interoperability as described in Figure 2 below. It is used in particular in the AIOTI White Paper on Semantic Interoperability (see [10]) as a starting point. This White Paper emphasizes in particularly the syntactic and semantic interoperability layers.

As a general observation, the more interoperability is supported at higher layer in the stack, the more the IoT systems will be provided with rich ways to interact with other systems.

![Figure 2: The AIOTI Interoperability Stack](image)

The AIOTI has considered the complete stack but grouped some of the layers and come up with a three layers functional model (as shown in Figure 3). This grouping is used in the HLA shown in Figure 1.

In short, the three layers have the following roles:

- **Application**: This layer contains the communications and interface methods used in process-to-process communications
- **IoT**: This layer groups some IoT specific functions (e.g. data storage and sharing); exposes those functions to the application via APIs; and makes use of the Network layer services.
- **Network**: the services of the Network layer can be grouped into data plane services, providing short and long-range connectivity and data forwarding between entities, and control plane services such as location, device triggering, Quality of Service (QoS) or determinism.
It is important to note that this three-layer architecture plays an important role in the analysis and scoping of the IoT platforms since most of their functionalities will be provided at the IoT layer where cross layer interoperability support will be required.

### 3.3.3 IoT-EPI White Paper patterns of IoT interoperability

IoT-EPI Task Force (where UNIFY-IoT was a key supporter) on Platforms Interoperability published a White Paper [14] entitled “IoT Platforms Interoperability Approaches - White Paper 2018”. It defines "Patterns of IoT interoperability" in the section 3.1.1 of the White Paper (and depicted in the Figure 3.2 of the White Paper not reproduced here to preserve authors’ rights).

To resume, we have five defined patterns of interoperability detailed in Figure 4 (text extract of the original White Paper [14]):

- Cross-Platform Access
- Cross-Application Domain Access
- Platform Independence
- Platform-Scale
- High-Level Service Facades
- Platform to Platform

The five patterns are:

- **Pattern I:** Cross-Platform Access
  It is the basic pattern where an application can interoperate with several platforms.

- **Pattern II:** Cross-Application Domain Access
  This pattern expands the previous with the ability to interoperate with platforms in different domains.

- **Pattern III:** Platform Independence
  The same application or service can be used on top of two different IoT platforms (e.g. in different regions) without changes.

- **Pattern IV:** Platform-Scale
  With this pattern, the focus is on integrating platforms of different scale.

- **Pattern V:** High-Level Service Facades
  This pattern extends the interoperability requirements from platforms to higher-level services where not only platforms but also services offer information and functions via the common API.

![Figure 3: The AIOTI Three Layer Functional Model](image)

**Figure 3:** The AIOTI Three Layer Functional Model

![Figure 4: Patterns of IoT interoperability defined in “IoT Platforms Interoperability Approaches White Paper 2018”](image)
CREATE-IoT and AIOTI WG03 shall consider this new IoT-EPI contribution to improve IoT Platform interoperability analysis and include this view in future interoperability recommendations to the address of IoT-LSP (Activity Group AG2 on “Activity Group 2 ("IoT standardisation, architecture and interoperability") and H2020 IoT LSPs running for 3 or 4 years from 2018 to 2010/2021.

3.4 High-Level (Reference) Architecture

The generic AIOTI three-layer functional model is reflected in the AIOTI HLA and serves the purpose of characterising the main elements of interaction between the devices (within the "Network Layer") and the applications (at the “Application Layer”) that are mediated by an "IoT Layer". This approach seems to evolve gradually over time and some new elements are creating the need for more layers in the IoT systems HLAs. One example of such element is the IoT virtualisation where IoT systems have to be structured in a way that can allow them to make use of Cloud based resources.

An example of such HLA is shown in Figure 5 (and more details for the functional architecture can be found in [8]). The horizontal layers are more than the three layers in the AIOTI HLA because of the need to represent (and separate with appropriate interoperability support) functions that can be provided whether locally or though one or more Cloud Service Provider (CSP). In this model, the IoT layer of the AIOTI HLA is split in several layers that group some functions with a growing level of abstraction from "cloud infrastructure" to "orchestration" with generic services provided on top of orchestration.

![Figure 5: A Virtualised IoT High-Level Architecture](Source ETSI TR 103527)

In addition to the horizontal layers, some vertical aspects addressing cross layers issues:

- Data Management that refer to the need of ensuring the coherence and integrity of the management of data across layers (considering, e.g., that the data can be managed also by edge computing devices);
- Management, in support of configuration, maintenance, operations, etc.;
- Security which needs to be dealt with globally in addition to the security services that are provided at a given layer (e.g., authentication and authorisation, etc.);
- Privacy and data protection, a growing need in IoT systems that needs to be catered globally also in order to ensure that the support to constraints such as the General Data Protection Regulation (GDPR) is complete and coherent.
The model above is rather generic and actual implementations of this kind of IoT systems may come up with slight variants. It should be noted that this model is also starting to emerge within some of the IoT Large-Scale Pilots.

3.5 Specific aspects

3.5.1 Semantic Interoperability

3.5.1.1 The rationale for Semantic Interoperability

Until recently, the focus of interoperability (in particular in standardisation) has been on technical interoperability (basic connectivity, network interoperability) and syntactic interoperability, largely based on Common Information Models offering static information (i.e. information based on a pre-defined syntax) to be exchanged. However, as soon as the requirement on the information exchanged become more complex (e.g., systems from different sectors), static information is no longer sufficient and the need arise for basing the exchange of information on its meaning (independently of underlying protocols): this is a scope and challenge of Semantic Interoperability. The challenge of Semantic Interoperability is that the meaning of semantics needs to be understandable and processed by machines. The most common way to achieve this is by using an ontology which is "an explicit specification of a [shared] conceptualization" (see [15]). Semantic Interoperability expands the goal of the Semantic Web which had proposed the evolution of the Internet from a web of documents to a web of machine-readable and understandable data. The IoT community has embraced this approach and the AIOTI has defined a framework for IoT Semantic Interoperability (see [10]) with the following conclusion (still valid, in particular regarding the support by IoT platforms): "[...] semantic approaches will expose many firms and individual engineers to new interoperability architectures and will require changes in tools, technologies, and thought processes."

3.5.1.2 The IoT Software Stacks

A typical IoT system – specially the latest ones making use of Cloud Computing solutions and resources – will encompass a variety of elements, devices, gateways and (potentially cloud-based) platforms. The implementation of such systems will rely on a limited number of IoT stacks. The model proposed by eclipse.org (see Figure 6) illustrates three typical stacks for constrained devices; for gateways and smart devices; and for cloud platforms.

Figure 6: The Three IoT Software Stacks
These stacks offer a growing level of functionality as the capabilities of the elements that run the stack is growing. They all use cross-stack functionality related to security (in particular for authentication, encryption, and authorization); development tools and Software Development Kits SDKs (supporting the different hardware and software platforms involved); and ontologies.

Ontologies are a key element in the support of interoperability: the format and description of device data is an important feature to enable data analytics and data interoperability. The ability to define ontologies and metadata across heterogeneous domains is a key area for IoT.

3.5.1.3 Semantic interoperability and the IoT stack

The IoT stack value proposition for IoT interoperability provides a good approach as well how to properly introduce semantic interoperability. It defines and establishes the relations between the operations and the role that “things” can play in an IoT system, alike the transformations that the data suffer from the basic process of data collection until it is used and exchanged as information and used to produce knowledge. Intermediate functions are also defined as part of an identified middle/mediation process in the stack.

![Semantic interoperability functional layers](image)

Figure 7: Semantic interoperability functional layers

Note: Figure 5 is sourced from DERI/Martin Serrano active in OpenIoT, IERC, AIOTI WG01 and WG03 and extracted from “InternetofThingsSession-SlidesMartinSerranoDERI.pdf” publicly available at [http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=7260](http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=7260) (Slide#24)

The main characteristics of the IoT Stack rely on the capacities of an IoT system to allocate functions and operations accordingly across those different layers:

- **At the physical level:** it is where raw data formats are handled and the collection, identification and handling of data relevant to a particular technology is performed.
- **At Sensor Middleware Level,** it is where data transformation is performed on moving time windows (expressed by time durations) to define useful data.
- **At Virtual Sensor Level,** it is where data aggregation on digital data is performed to identify, mark and classify useful data, information that is useful for control and provisioning applications and also services deployments is usually added at this level. As consequence of this aggregation parts of a vocabulary must be used and universally used.
- At the Semantic Level, it is where data management tools are provided to query information and offer intermediate access from application to data by means of linked data. At this level, knowledge database or repositories for data and annotations reside and other vocabularies and ontologies.
- At the Application Level, it is where data formal representations reduce the burden of performing common aggregation, thereby boosting specific representations and reducing ambiguity in a trade-off manner with complexity. At this level, all the data can be offered by means of standard open software interfaces or tailored for specific domains.
- At the Business Level, it is where provisioning and visualizations for end users are offered as service. In this level domain-specific representation has non-technological dependency and majorly data is driven in the form of aggregated services.
- At the organisational level, it is where the OpenIoT Stack contains the general interoperability process that rely more in “intelligence” services provided as information services, and as result of statistical and analytical processes.

3.5.1.4 Usage of semantics at different levels of the architecture

It is expected that semantic technologies offer outstanding features in support of essential requirements of the IoT infrastructure, including discovery, interoperability, consistency, scalability, reusability, composability and automatic operations of data and services. To this extent, semantic technologies are applicable to the different functional layers of the IoT infrastructure.

IoT high level architecture model

![Figure 8: Applicability of semantic technologies to IoT HLA layers](image)

Taking as reference the layers identified in the (current version of the) AIOTI WG03 HLA model, Figure 8 outlines that semantic technologies can provide added value at all layers:
- At Application layer, semantic technologies can help to provide users with a smart HMI (Human Machine Interface);
- At IoT capabilities layer, semantic technologies can help the discovery and automatic interoperation of the capabilities and resources deployed in distributed nodes (e.g. devices, gateways, servers);
- At Network layer, the semantic technologies can simplify and help to automate the network configuration.

Similarly, semantic technologies can also offer added value to some of the layer-cutting (“vertical”) issues identified in Figure 5 (A Virtualised IoT High-Level Architecture Source ETSI TR 103 527)
- From a device perspective, semantic technologies can help the IoT infrastructure understand the properties of devices, e.g., computation or storage capacity, type of sensor etc.
- From a security perspective, semantic technologies can improve security-related decision-making (e.g., role-based access rights). Furthermore, semantic technologies can enhance the
conventional description of security policies, thus helping the security negotiation process between different technical components of the IoT.

- From a management perspective, the semantic technologies can facilitate machine-based understanding of service logs and support the automatic configuration of the technical components of the IoT system.

3.5.1.5 Some examples

**oneM2M**
The purpose and goal of oneM2M is to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide.

In oneM2M application data are stored under resources. Specific resource types (application, containers, etc.) may have a semanticDescriptor resource that describes the semantic meaning of the data aka “Semantic Annotation” according to a given ontology. Such semantic description allows for:

- Semantic discovery: enhancing the discovery mechanism, to allow locating and linking resources or services based on their semantic information;
- Semantic reasoning: derive new relations and classifications of semantically annotated data;
- Semantic mash-up: create new virtual devices and offer new services.

This is specified in oneM2M TS 0012 "oneM2M Base Ontology" that

- Contains the specification of the oneM2M base ontology (http://www.onem2m.org/ontology/Base_Ontology)
- Specifies an instantiation of the base ontology in oneM2M resources which is required for generic interworking.
- Contains the functional specification for an Interworking Proxy Application Entity (IPE), the oneM2M resources and their usage for generic interworking
- Contains an example is given how external ontologies can be mapped to the base ontology. The example uses the Smart Appliances REFerence (SAREF) ontology (http://ontology.tno.nl/saref).

**OpenIoT**
In OpenIoT a well-defined semantic-based model representation is the result of the related existing vocabularies in the area of IoT. The vocabularies are formally represented using ontologies and by the nature of the OpenIoT services-web orientation the language used is OWL (Ontology Web Language).

OpenIoT follows the common and desired approach to reuse existing ontologies as much as possible, simplifying the development since one can focus at the domain or application-specific knowledge only, and, the integration between applications in the future since defined parts of ontologies will be shared.

**SAREF**
The Smart Appliances/Applications REFerence ontology (SAREF) is the result of an EU initiative launched in 2013 with the support of ETSI in order to create a shared semantic model based on consensus to enable the missing interoperability among smart appliances. SAREF can be considered as an addition to existing communication protocols to enable the translation of information coming from existing (and future) protocols to and from all other protocols that are referenced to SAREF. For example, a home gateway enriched by SAREF can associate devices in a home with each other and with different service providers.
The initial focus was on the optimisation of energy management in smart buildings. The first resulting semantic model – SAREF – was standardized by ETSI in November 2015 (TS 103 264, see [11]). SAREF is a first ontology standard in the IoT ecosystem, and sets a template and a base for the development of similar standards for other verticals. Since its first release, SAREF continues to evolve systematically into a modular network of standardized semantic models, with three additional extensions: SAREF for Energy, SAREF for Environment and SAREF for Buildings. Work is on-going in a number of other domains such as Smart Cities, Smart AgriFood, Smart Industry and Manufacturing, Automotive, eHealth/Ageing-well and Wearables. The objective is to make SAREF a “Smart Application REFerence ontology”, which enables better integration of semantic data from various vertical domains. SAREF is more detailed later in the present document.

W3C
W3C’s vision for the Web of Things (WoT) focuses on the role of Web technologies for a platform of platforms as a basis for services spanning IoT platforms from microcontrollers to cloud-based server farms. Shared semantics are essential for discovery, interoperability, scaling and layering on top of existing protocols and platforms.

For this purpose, metadata can be classified into: things, security and communications, where things are considered to be virtual representations (objects) for physical or abstract entities. Things are defined as having events, properties and actions, as a basis for easy application scripting. This assumes a clean separation between the application and transport layers, which simplifies scripting by decoupling the details of protocols and message formats, allowing servers to use the protocols that best fit the particular context. Communications metadata allows servers to identify how to communicate with other servers.

Thing descriptions are expressed in terms of W3C’s resource description framework (RDF). This includes the semantics for what kind of thing it is, and the data models for its events, properties and actions. The underlying protocols are free to use whatever communication patterns are appropriate to the context according to the constraints set by the given metadata. W3C is exploring the use of lightweight representations of metadata that are easy to author and process, even on resource constrained devices.

3.5.2 Marketplaces and APIs
A new breed of IoT systems based on layered, potentially cloud-based or edge-enabled architectures is emerging with strong requirements on the connectivity between actors (e.g., sensors, gateways, platforms, data processing and analytics functions, etc.) that require complex interoperability schemes, as seen in section 3.3.

In this new world, IoT systems and application developers would expect that the myriad of devices that are deployed and connected to the network can seamlessly interoperate with a large range of platform services (e.g., data analytics, monitoring, visualisation, etc.) and end-user/end-customers applications. With the use of the proper services, useful data and information can be exchanged between all actors across the system.

In this model, the actors can be seen as consumers and providers within an emerging application market. An IoT marketplace is a new platform to extend the "traditional" IoT platforms with brokerage concepts supporting automated discovery, trading and even pricing. Within an IoT marketplace platform, the IoT device owners will have the possibility to selectively grant access and trade their data with many potential vendors thus creating an environment where innovative
solutions can be monetised (and efficiently developed) in support of a multi-vendor and multi-owner environment.

The marketplace architectures are in general supported by:

- The publication of a number of Application Programming Interfaces (APIs) that hide the actual underlying provision of the service from the consumer of the service. The implementation of the service can change without impacting the rest of the system and the evolution of the APIs can be mastered via the publication mechanism;
- An approach based on Micro services where any service (whichever its size and scope) can be published and consumed. This approach provides system flexibility; supports lean software principles; and allows fast adaptation to support emerging standards without impacting the whole system architecture.
4. THE IoT PLATFORMS AND THE STANDARDS FRAMEWORK

4.1 Introduction
The standards framework described in section 3 has outlined the main elements (HLA, horizontal and vertical maps, interoperability patterns, semantic interoperability, security, etc.) that IoT systems architects, designers and developers may use for the most up-to-date identification of the support that standardisation has brought to the IoT community. This section briefly characterises with practical details how these standards can be identified, classified and used, with a particular focus on interoperability. Moreover, a list of around 50 IoT platforms is identified with, for some of them, a discussion on how they support the standards (interoperability) framework.

4.2 IoT Standards
The IoT Standards are constantly evolving in number, in scope, in application domains, etc. It is important to know which Standards are applicable to the IoT community. There are two kinds of such standards:
- Standards that are IoT-specific and have been or are being developed within SDOs or SSOs that deal specifically with IoT issues. The SDOs and SSOs involved can be general purpose and have IoT-specific working groups;
- General purpose standards than can apply also to the IoT domain. A good example of such standards are the security standards: most of these standards are developed for a large range of systems, possibly without any IoT part.

The AIOTI Working Group 3 on IoT Standardisation has developed an IoT landscape using the distinction between the horizontal and vertical domains (see 3.2.1) for the classification of the organisations that are active in IoT standardisation. The classification of IoT standardisation organisations has been done along two dimensions:
- Vertical domains representing 8 sectors where IoT systems are developed and deployed;
- A “horizontal” layer that groups standards that span across vertical domains, in particular regarding telecommunications.

In order to give an indication of the relative importance of “horizontal” versus “vertical” standards, the ETSI report on the IoT Landscape (see [5]) has identified 329 standards that apply to IoT systems. Those standards have been further classified in:
- **150 “Horizontal” standards**, mostly addressing communication and connectivity, integration/interoperability and IoT architecture.
- **179 “Vertical” standards**, mostly identified in the Smart Mobility, Smart Living and Smart Manufacturing domains.

The list is changing (mostly growing over time). An example of how the list of applicable standards is growing is the development of IoT Virtualisation which adds to the above-mentioned list a number of Cloud Computing standards.

4.3 IoT Platforms

4.3.1 Introduction
There are potentially hundreds of IoT platforms available for the development of IoT systems, ranging from point solutions managing a part of the IoT stacks up to very general purpose that integrate the IoT system as a component in a larger system (e.g., enterprise systems). These platforms have very different coverage, different development status, user adoption level.
Moreover, they can also have very different support to interoperability and to the standards in support of it.

So, the question of the choice of platform(s) by IoT system designers, developers and validators may turn out to be very complex. It is very often complicated by the existence of a legacy system that may demand the use of another set of platforms. Even if there is no silver bullet, the approach that can be taken is that of identifying criteria for defining the relevance of IoT platforms and evaluate how a given platform meets these criteria. The approach of evaluation and scoping has been used within the IoT Research and Innovation community with two complementary activities:

- The analysis of the platforms used in the IoT-EPI projects. **This has led to the identification of 34 platforms** that are in use within the IoT-EPI projects.
- The analysis of general technical literature done in UNIFY IoT Work Package 3 with the purpose of identifying a list of platforms that are generally considered as meeting a number of the criteria listed above (see [2]). **This has led to the identification of 19 platforms.**

The platforms identified by the above-described analysis are presented in the rest of this section.

### 4.3.2 The platforms in the IoT-EPI Projects

#### 4.3.2.1 The different requirements and approaches in the IoT-EPI projects

The IoT-EPI projects are developing various interoperability solutions that 1/ address different layers in the IoT architecture; and 2/ offer mechanisms for providing interoperability between different IoT platforms (see [14]).

More specifically:

- **AGILE** builds a modular hardware and software gateway for the IoT focusing on the physical, network communication, processing, storage and application layers.
- **bIoTope** provides an architecture and recommendations for the use of open standards; develops and provides standardised open APIs to enable interoperability.
- **BIG IoT** develops a generic, unified Web API for IoT platforms, focussing on the upper layers of the IoT architecture and addressing the security management, APIs, service integration, external system services, applications, and the business enterprise.
- **INTER-IoT** addresses an open cross-layer framework, an associated methodology and tools to enable voluntary interoperability among heterogeneous IoT platforms, focusing on modules for QoS and device management, service integration, external system services, storage and virtualisation.
- **symbIoTe** is providing an abstraction layer for a unified view on various IoT platforms and sensing/actuating resources, implementing a semantic IoT engine to find adequate resources.
- **TagItSmart!** offers a set of tools and enabling technologies integrated into a platform with open interfaces, offering modules for security management, business logic, service integration, storage, APIs, big data analytics and business enterprise.
- **VICINITY** focuses on a platform and an ecosystem that provides “interoperability as a service” for infrastructures in the IoT, considering service integration, business logic, virtualisation, storage, APIs, tools, external system services, applications, data analytics and cloud services.

#### 4.3.2.2 The platforms in the IoT-EPI projects

The IoT-EPI projects are in general embedding several platforms that are described in more details in the appendices.

The Table 1 below is listing the platforms used by the various. It can be noted that some of them are used across several IoT-EPI projects (highlighted in bold).
<table>
<thead>
<tr>
<th>Project</th>
<th>IoT Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGILE</td>
<td>Eclipse IoT, NodeRED, Resin.io.</td>
</tr>
<tr>
<td>bIoTope</td>
<td>DIALOG, eAir web, FIWARE, Mist, NodeRED, O-MI/O-DF Reference Implementation, Open IoT, Warp 10</td>
</tr>
<tr>
<td>BIG IoT</td>
<td>BEZIRK, Bitcarrier/Sensefield/FastPrk, Open IoT, Smart City Platform, Smart Data Platform, Traffic Information Center, Wubby</td>
</tr>
<tr>
<td>INTER-IoT</td>
<td>AWS, Azure, e-Care Tilab, Eclipse OM2M, FIWARE, I3WSN, NodeRED, Open IoT, SEAMS, Unical BodyCloud, UniversAAL</td>
</tr>
<tr>
<td>symbIoTe</td>
<td>KIOLA, MoBaaS, nAssist, Navigo Digitale IoT, Open IoT, Symphony</td>
</tr>
<tr>
<td>TagItSmart</td>
<td>Evrything, FIWARE, RunMyProcess, SocIoTal</td>
</tr>
<tr>
<td>VICINITY</td>
<td>IoTivity, LinkSmart</td>
</tr>
</tbody>
</table>

Table 1: Platforms used by the IoT EPI Projects

In total, 34 different platforms are used by the 8 IoT-EPI projects referenced.

4.3.3 The platforms identified by UNIFY-IoT

UNIFY-IoT has been working on the criteria for the selection of "leading platforms" in the IoT ecosystem (see [2]). Based on a variety of sources, they have extracted a list of 23 IoT platforms that are seen as having more relevance to the IoT community (industry, research, etc.) as a whole. These platforms have been analysed in more depth (in [2]).

4.3.4 Other platforms

In addition to the above listed platforms, the Table 2 presents some platform originating from the Telecommunications sector.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Provider</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirVantage</td>
<td>Sierra Wireless</td>
<td><a href="http://www.airvantage.net">www.airvantage.net</a></td>
</tr>
<tr>
<td>SensorLogic</td>
<td>Gemalto</td>
<td><a href="http://www.gemalto.com/m2m/solutions/application-enablement">http://www.gemalto.com/m2m/solutions/application-enablement</a></td>
</tr>
</tbody>
</table>

Table 2: Telecommunications Originated Platforms
4.4 Standards and support of interoperability in IoT platforms

4.4.1 Introduction
Amongst the platforms identified above, some - the platforms of the IoT-EPI projects - have addressed the description of the kind of support they provide to interoperability and, to some extent how the support the standards framework described above. A summary of their findings is described in this section, with a focus on Semantic Interoperability when possible (for more see [14]).

4.4.2 Examples of interoperability support in IoT-EPI projects

4.4.2.1 Interoperability in the BIG IoT platform
The BIG IoT main architectural concepts rely on the notion of marketplace as a mediation between providers and consumers of resources. Four interfaces to the marketplace are provided that support the five patterns of interoperability described in the IoT White Paper [14].

The main challenge for supporting the IoT EPI White Paper interoperability patterns II, III, and V is that they target interoperability among highly heterogeneous entities, such as:

a) Resource providers and consumers from different verticals or application domains (II);
b) Resource providers hosted on different IoT platforms, e.g. located in different regions (III);
c) Resource providers on different provider systems, e.g. an IoT platform or a service (V).

To bridge the interoperability gap for those patterns, the architecture mandates the use of a Core Information Model (CIM), such as the one provided by the Semantic Web and Linked Data. Providers (of platforms or services) use CIM to describe the resources they offer in a machine understandable manner, so that consumers (services/applications) of a different domain, region or system can understand and process them. For example, Schema.org vocabularies are the shared common understandings between search engines and billions of web pages.

The CIM are also used by the marketplace to match the supplies and demands of providers and consumers: data providers and data consumers can share the same vocabularies for entities such as “smart object”, “sensor”, “measurement”, etc. in the same way that search engine providers agree with Web developers how to describe “restaurant”, “hotel”, “airline”, etc.

Consumer and Provider Libraries (Libs) are another important element of the architecture: they implement functionalities of the ecosystem. For example, the Provider Lib implements the Register interface (M2) to offer resources via the marketplace and offers the Access interface (A1) to provide the information to a consumer. The benefit for developers of platforms, services and applications is that they only have to implement once the Provider (P1) or Consumer (P2) interface and can easily update the libraries in order to further comply in case of changes in the details of the underlying message formats and interactions.

4.4.2.2 Interoperability in the bIoTope platform

Architecture
The architecture of bIoTope supports the provision advanced Systems-of-Systems (SoS) capabilities for connected smart objects in order to enable to easily create new IoT systems. This architecture is not as layered architecture as regards the physical size or computational capabilities of the communicating systems.

bIoTope comes with a set of supporting standards:

- Any system that implements the set of supporting IoT standards can communicate directly with any other system that implements and understands the same standards;
• Systems that do not natively support the necessary IoT standards can join by using "wrappers", i.e. software components that expose the services as they should be published if they supported the appropriate standards. Data and services that are not public remain non-accessible to unauthorized parties.

The bloTope architecture is heavily influenced by an approach based on Microservices: a service of any size can be published and consumed. This approach provides system flexibility; supports lean software principles; and allows fast adaptation to support emerging standards without impacting the whole system architecture.

**Standards support**
In bloTope, the IoT standard refers to a limited set of appropriate standards around the “waist” of the standards landscape with the core IoT standards outlined in bold. The other standards are used depending on the different domains and different requirements from different applications. When other standards (or proprietary protocols and formats) than the core IoT standards are used, bloTope uses a Wrapper for making them compliant with the core IoT standards.

To this end, bloTope takes full advantage of messaging standards developed and officially published by The Open Group, notably the Open Messaging Interface (O-MI) and Open Data Format (O-DF) standards. O-MI provides a generic Open API for implementing RESTful IoT information system (using other underlying protocols than HTTP).

In the bloTope ecosystem, different systems compliant with the IoT standard support (through Wrappers or not) are made aware of each other’s existence and the different data and services that they provide to each other. When a new system needs to "join", bloTope will provide mechanisms for discovering relevant O-MI nodes. Certain nodes will implement the bloTope IoTBNB API, which is a marketplace for IoT compliant services.

4.4.2.3 Interoperability in the Inter IoT platform
INTER-IoT offers a layer-oriented solution to allow interoperability between IoT platforms and systems at different layers. This solution is based on both an open framework (INTER-FW) and a methodology (INTER-METH) and it can be applied within any application domain and across several domains. The INTER-IoT approach has interoperability benefits: it facilitates a tight bidirectional integration; high performance; complete modularity; high adaptability and flexibility, and is expected to support increased reliability.

INTER-IoT benefits can be reaped at different levels, in particular regarding the Data and Semantics level: a common interpretation of data and information from different platforms and heterogeneous data sources, providing semantic interoperability.

The INTER IoT layer-oriented solution is achieved through several interoperability solutions dedicated to specific layers (e.g., Device-to-Device, Networking-to-Networking, Application & Services-to-Application & Services; Data & Semantics-to-Data & Semantics).

Each interoperability infrastructure layer has a strong coupling with adjacent layers and provides an interface. The interfaces are controlled by a meta-level framework to provide global interoperability. Every interoperability mechanism can be accessed through an API. The interoperability infrastructure layers can communicate and interoperate through the interfaces.

In particular, the INTER-IoT solution for the Data and Semantics layer allows a common interpretation of data and information among different IoT systems and heterogeneous data sources, thus supporting semantic interoperability. It is based on semantic translation of IoT platforms ontologies to/from a common modular ontology.
4.4.2.4 Interoperability in the symbIoTe platform

symbIoTe addresses the creation of an interoperable IoT ecosystem that supports the collaboration of vertical IoT platforms for the creation of cross-domain applications. To this extent, it offers an interoperable mediation framework to enable the discovery and sharing of connected devices across existing and future IoT platforms for rapid development of cross-platform IoT applications.

Syntactic and semantic interoperability represent the essential interoperability mechanisms in the symbIoTe-enabled ecosystem. Organizational interoperability has different flavours (platform federations; dynamic smart spaces; and roaming IoT devices) to enable platform providers to choose an adequate interoperability model for their business needs.

The symbIoTe architecture is built around a layered IoT stack connecting various devices (sensors, actuators and IoT gateways) within smart spaces with the cloud. Smart spaces share the available local resources (connectivity, computing and storage), while platform services running in the cloud enable IoT Platform Federations (associations between two platforms) and open up the Interworking Interface to third parties.

The architecture comprises four layered domains, 1) Application Domain, 2) Cloud Domain, 3) Smart Space Domain and 4) Device Domain

Four different Compliance Levels (CLs) for IoT platforms which reflect different interoperability modes that an IoT platform can support. Those different interoperability modes affect the functionality which has to be supported by symbIoTe-enabled platforms, and require specific symbIoTe components to be integrated within different domains.

symbIoTe addresses semantic interoperability. Two existing IoT platforms expose platform-specific APIs (based on an internal information model) to applications. symbIoTe is placed between those two vertical IoT stacks, with the Core Information Model (CIM) at the centre. CIM describes general concepts and relations that are shared between all platforms whereas the Meta Information Model describes symbIoTe internal meta-data about platforms and resources. For a platform to become symbIoTe-compliant, it must expose its data using a platform-specific information model, which is a platform-specific extension of the CIM.

The main part of the actual interoperability between the two platform-specific information models: a semantic mapping. This allows to define how the platform-specific extension of one platform can be translated into the platform-specific extensions of another. When an application or a platform queries the Core API to find resources of interest on all available platforms, symbIoTe uses these mappings to re-write the query to fit the platform-specific information model of each platform and execute it against the meta-data it has stored about each of them.

4.4.2.5 Interoperability in the TagItSmart platform

At the Service level, the following functional blocks can be found in the TagItSmart platform:

- **Security** deals with e.g., components authentication, authorisation and access control;
- **Service Execution** supports the execution of services registered in the platform, as well as the service templates that will trigger dynamic creation of workflows;
- **Data Processing** components handle and work with the data generated in the platform;
- **SmartTags** components facilitate the integration, creation and scanning of SmartTags;
- **Data Access** components provide the registries, semantic models and repositories.

Each component is intended to define an integration strategy, mainly by the definition of an Open API. In the platform, a reference implementation is provided for the core innovative components...
(i.e. all the components directly related to the SmartTags and services), while others are taken/integrated from already existing platforms.

Based on the chosen integration strategy, the mapping of some of the components to real implementations and deployments in a specific IoT platform will be different. However, TagItSmart components define a common API to guarantee interoperability and seamless integration, as well as enabling the creation of third party applications on top of these components.
5. ETSI SMARTM2M AND ONEM2M

5.1 Introduction

ETSI Groups have already well detailed (in UNIFY-IoT deliverables, IoT Cluster Book…) radio interoperability framework of 3GPP e.g. (4G/LTE-M, 4G/NB IoT) and IoT service-layer interoperability framework of oneM2M. This is a must to improve the awareness of the benefit of these radio and service global interoperable standards. ITU SG 20 recent endorsement of oneM2M standards correspond exactly to this need and recognition. CEN and CENELEC are partner type 2 of oneM2M.

The detailed information presented hereinafter are showing that IoT application/data interoperability gap (with other Applications/Services/Platforms/Middleware) can now be filled by IoT Semantic interoperable standards thanks to available Release 2 of oneM2M interoperability framework and architecture (at least via Mca oneM2M application interface). IoT Base Ontology of oneM2M is the core of the IoT Semantic Interoperability (SemIoP) that gained momentum with AIOTI WG03 IoT SemIoP activities and IoT common High Level Architecture definition and agreement.

EC funded studies on SAREF (initially expanded to Smart Appliance REFerence ontology) were in the beginning, dedicated to Smart Appliance and created an unexpected momentum and credibility of IoT SemIoP. Today SAREF is known as a Reference ontology mapped in main IoT Domains and anchored to oneM2M IoT Based Ontology (and interoperable framework). SAREF is now expanded to Smart Applications REFerence ontology.

But, the question is why aren’t we all adopting these worldwide recognized standards if it is so obvious?

It became obvious that, except with 3GPP (www.3gpp.org), the battle to interoperate globally at protocol levels (under the service layer) is so fragmented that the need for interworking led to the creation of an international partnership “like GSM” (with quite the same international partners) gave the birth to oneM2M partnership project (www.oneM2M.org) where all regional SDOS decided to choose one and only one M2M/IoT standardised set of interfaces (device, gateway, server, application and services-to-application, services-to-services) at the service layer.

Note: oneM2M, like 3GPP, is an ETSI Partnership Project (EPP) whose partners (different from 3GPP) http://www.onem2m.org/about-onem2m/partners are:

- **oneM2M type 1 partners:** ARIB (Japan), ATIS (US), CCSA (China), ETSI (Europe), TSDSI (India), TTA (Korea), TTC (Japan) that are in common with 3GPP plus TIA (United States)
- **oneM2M type 2 partners:** BBF (Broadband Forum), CEN, CENELEC, GlobalPlatform and OMA.

Once deciding to develop middleware, services, application complying the provider independent, standard based framework of oneM2M this is possible to envisage to develop and deploy interoperable IoT services and application able to inter-operate via common oneM2M standards.

So oneM2M interoperability framework (interfaces) and the principles of IoT Semantic Interoperability can be added “inside” IoT Platforms without putting into question any existing feature. oneM2M and SemIoP offer opportunity to draw additional/extended strategic interoperability plans. oneM2M is an interoperability standard framework! Even if it looks more complex at first sight than single solutions approaches (not potentially broadly interoperable by design), the complexity aspect is easy to catch because interoperability by design includes many
additional and different heterogeneous scenarii (when including for instance oneM2M Partners type 2 and organisations with oneM2M cooperation agreements) but also when using oneM2M Mca interface to applications. This oneM2M Mca interface is key for SemIoP, for example ETSI ISG CIM “cross cutting Context Information Management” is developing an NGSI-LD standard (endorsed by GSMA, TM Forum and FIWARE NGSI) based on Mca.

To cope with the apparent complexity of the oneM2M interoperability framework, there are OSS oneM2M based reference implementations available for free on the shelves (like http://www.eclipse.org/om2m/) and that are possibly useful to be re-used it in coding and to conduct interoperability testing.

This is now more a question of awareness and pace of adoption. Even the best “norm” in the world needs time and sometimes fails to be well understood, recognized, implemented and generalised to become a “standard” for interoperability.

5.2 SAREF Rationale

ETSI SmartM2M (ETSI is partner of oneM2M) tackles IoT, interoperability, and Semantic Interoperability challenges, contributing to the digital transformation of industry sectors in Europe. The SAREF standard ontology is a key flagship to reach semantic interoperability in IoT and Web-based applications where digitized assets play a central role

SAREF is an ETSI standard (TS 103 264 V2.1.1 published in March 2017 including also TS 103 410-1 (SAREF4ENER)/Energy Domain, TS 103 410-2 (SAREF4ENVI)/Environment Domain, TS 103 410–3 (SAREF4BLDG)/Buildings Domain, TS 103 67 (Smart Appliances Application of oneM2M Communication Framework) and the related testing suite in TS 103 268-1,-2, -3 and -4.

Smart Appliance REFerence ontology (SAREF) was originally created in a standardization initiative launched by EC DG CNECT, conducted in collaboration with ETSI TC SmartM2M. The EC, as a first step, identified an immediate market need to reduce the energy utilization by managing and controlling Smart Appliances (for example, in a house or an office building) at a system level. In particular, Industry and the EC raised the need for a common architecture with standardized interfaces and a common data model to assure interoperability. Without these two components, the current market landscape would continue to be fragmented and to lack efficiency. Therefore, the development of a reference ontology was targeted as the main interoperability enabler for appliances relevant for energy efficiency, and ETSI has accepted to cover the communication aspects and to provide the necessary standardization process support.

As a result, following a broad consultation with stakeholders to address clear market needs, the EC financially supported a study to create a language (so-called ‘reference ontology’) for smart appliances. TNO was in charge of performing the study to create the first version of this reference ontology (SAREF), which was completed on April 1st, 2015. The outcomes were then transferred to ETSI, to turn the material into a Technical Specification. This task was executed by ETSI TC SmartM2M, and the first specification version was published in November 2015 (TS 103 264 V1.1.1).

This ETSI specification defines a new reference conceptual language for energy-related applications. This language will be used by devices at home (from lamps and consumer electronics to white goods like dishwashers) to allow them to exchange information with any energy management system, which could physically be in the home or in the cloud.
SAREF will foster demand-response to flourish, will bring additional energy and cost savings for building owners and users, and will favour emerging markets. The intention is to build on converging standardization work and on the development of open platforms on which technologies and solutions will co-exist and interact across application domains.

This is why ETSI TC SmartM2M proposed to extend the SAREF standard taking into account:

- **Automotive domain use cases and available existing data models**, in close collaboration with AIOTI, the H2020 Large Scale Pilots (e.g. AUTOPILOT), ETSI and oneM2M.

- **eHealth/ Ageing-well domain use cases and available existing data models**, in close collaboration with AIOTI, the H2020 Large Scale Pilots, ETSI (in particular EP eHealth and TC SmartBAN) and oneM2M.

- **Wearables domain use cases and available existing data models**, in close collaboration with AIOTI, the H2020 Large Scale Pilots, ETSI (in particular TC SmartBAN) and oneM2M.

- **Water domain use cases and available existing data models**, in close collaboration with AIOTI, the H2020 Large Scale Pilots, results of the projects from the ICT4WATER cluster, ETSI and oneM2M.

To that end, in 2018, an ETSI TC SmartM2M will produce four Technical Reports (TRs), one for each domain (i.e., Automotive, eHealth/ Ageing-well, Wearables and Water domains), with the aim to determine the requirements from the considered domains, collect use cases and identify available existing data models. Moreover, TC SmartM2M will produce 4 Technical Specifications (TSs), one for each domain, with the scope to specify an initial extension to SAREF for each of these domains based on the requirements expressed in the corresponding TR.

It is of particular importance that, for identifying the requirements and defining the extensions in these domains, the stakeholders in the related domains are consulted and actively involved to ensure that the extension is supported from the start of its development.

A coordination with major activities in the semantic interworking context is envisaged by TC SmartM2M, in particular with STF 534 (SAREF extension for smart cities, smart agrifood and smart industry and manufacturing).

**In 2018, ETSI TC SmartM2M will leverage SEAS project outcomes to improve SAREF mapping tools and methodology in the Energy Sector (and other domains).**

SEAS is an EUREKA ITEA 12004 SEAS (Smart Energy Aware Systems) project. It was made of 35 partners with a total budget of 13.5 M€. The SEAS project ran from February 2014 to December 2016 (https://itea3.org/project/seas.html), and received the ITEA Award of Excellence 2017. Its goal was to design and develop an eco-system of smart things and services, collectively capable of optimizing the energy efficiency within the future Smart Grid. SAREF focuses on the notion of device, while industry use cases often require some description of the physical systems and their connections, value association for their properties, and the activities by which such value association is done. The SEAS ontology is a modular and versioned ontology with all the terms it defines having the same namespace (https://w3id.org/seas/). Ontology patterns are like design patterns in object oriented programming. They describe structural, logical, or naming, best practices that one can consider when building an ontology. The SEAS ontology contains a core of SEAS reference ontology patterns that can be instantiated to create the SEAS ontology itself with a homogeneous and predictable structure for the modelling and the description of any kind of engineering-related data/information/systems. TC SmartM2M will consolidate the SAREF ontology adapting the SEAS strategy, and filling some of the representational gaps that were identified.
Despite of the success and the good initial footprint of SAREF, TC smartM2M still have to support the vertical business players (in this case the energy providers and distributors) that have not yet developed the necessary competences on SAREF, oneM2M and more in general on ontologies and semantic interoperability.

The remaining part of TC SmartM2M work is to facilitate the inclusion and self-contribution of the actors from the different vertical business sectors (not only the energy one, but starting from the energy one) by creating tools (portals, feedbacks and bug reporting, etc) and procedures to enable these actors to provide their feedbacks and proposals.

The value of SAREF is strongly correlated with the size of its community of users, and ontologies must be available on the Web. As such, SAREF users’ community and the industry actors need to be attracted to SAREF with clear documentation and a clear indication about how to provide their input and the kind of input that they can supply.

The final TC SmartM2M objective is to make the business community able to provide their input to SAREF and to maintain SAREF without the need of a special support from ETSI, but just with revisions from the ETSI members, and in particular from TC SmartM2M.
6. ETSI SMART CITY

6.1 Introduction
In ETSI, TC SmartM2M is cooperating with ETSI TC SmartBAN (Smart Body Area Networks) and ISG CIM (cross-cutting Context Information Management) to develop complementary and integrated components to oneM2M and to avoid overlap with oneM2M and standards fragmentation.

Two concrete examples of TC SmartM2M SAREF and ETSI ISG CIM cooperation in the Smart City domain are:

- **DTR/SmartM2M-103506 (TR 103 506)** “SmartM2M; SAREF extension investigation; Requirements for Smart Cities” where the scope is to determine an initial semantic model for Smart Cities based on a limited set of use cases and from available existing data model. This work is expected to be developed in close collaboration with AIOTI, the H2020 Large Scale Pilots and with ETSI activities in the smart cities, primarily ISG CIM and ISG CDP Use Cases and related semantic model are expected to be aligned with corresponding work in ISG CIM. Further extensions are envisaged in future to cover entirely the smart cities domain.

- **DTS/SmartM2M-103410-4-SRF4CITY (TS 103 410-4)** “SmartM2M; Extension to SAREF; Part 4: Smart Cities Domain”.

6.2 Smart City IoT interoperability

**SAREF, oneM2M IoT Base Ontology, ISG CIM/NGSI-LD and AIOTI WG03/SemIoP**

From digitizing of industrial processes to creation of smart services for citizens, it is essential to accurately record data together with its context information, the so-called meta-data, and to transfer these without misinterpretation to other systems. Single-purpose solutions (e.g. measuring temperature at a weather station) work well within a known/pre-set context, but transfer of the data to another system (e.g. personal travel planner) or another country (e.g. from UK to France) requires pre-agreed standards.

A century of international collaborations has achieved thousands of such agreements, but technologies such as Big Data, semantic web, Linked Data, autonomous decision making and eGovernment are enormously forcing the pace. The ETSI ISG (Industry Specification Group) on cross-cutting Context Information Management (ISG CIM) is developing Group Specifications (GSs) for applications to publish, discover, update and access context information, initially for a broad range of smart city applications, later for other areas.

In 2017, the work progressed well in ISG CIM on five work items. These include the collection and analysis of use cases, the identification of a general architecture and an analysis of the huge range of existing guidelines, standards and context information formats. An initial definition of a flexible information model was agreed, which is compatible with linked data, Internet of Things and relational databases. A preliminary version of an Application Programming Interface to enable almost real-time access to information coming from many different sources (in addition to the IoT) was completed Q1 2018. The final ETSI ISG CIM API will be referred to as NGSI-LD in agreement with OMA and will be endorsed by GSMA, FIWARE NGSI and TM Forum.

The ETSI ISG CIM has already benefited from advice of experts in ETSI SmartM2M, oneM2M, W3C Web-of-Things and (during an open workshop and via contributions from members) from a number of relevant H2020 projects. The next steps involve collaborations with other SDOs and
experts to facilitate the best possible interworking between existing widely used systems, as well as to take account of provenance, security and privacy issues. As a matter of policy, introductory and intermediate material is regularly made publicly available in the ETSI open area (https://docbox.etsi.org/ISG/CIM/Open). ETSI ISG CIM API (published Group Specification/GS CIM 004 “Context Information Management (CIM); Application Programming Interface (API)” is the precursor of ETSI ISG CIM NGSI-LD API (GS CIM 009 “Context Information Management (CIM); NGSI-LD API “). The new ETSI ISG CIM work item DGS/CIM-009 on CIM NGSI-LD API has been initiated to encompass any necessary changes/improvements to the preliminary API GS CIM 004. In ETSI ISG CIM API Group Specification developments, the text string “NGSI-LD” will be used, with the formal agreement of OMA which originally defined NGSI. This will greatly help in avoiding confusion with the IEC CIM/Common Information Model specifications. ETSI ISG CIM adopted the following general definition of “Context Information”: any information that can be used to characterize the situation of one or more entities and which is considered relevant to the interaction between a user and a service (e.g. software application), and other data elements, including the user and the service themselves. ISG CIM has a policy of openly publishing intermediate material (as soon as consensus is reached) to enhance feedback. Where possible the material is also presented at public technical events to engage with the community.

6.3 Core objectives of TC SmartM2M, TC SmartBAN and ISG CIM

ETSI TC SmartM2M has primary responsibility
- To provide specifications for M2M services and applications. Much of the work focus on aspects of the Internet of Things (IoT), Smart Appliances and Smart Cities;
- To support European policy and regulatory requirements including mandates in the area of M2M and the Internet of Things; to include in its work the identification of EU policy and regulatory requirements on M2M services and applications to be developed by oneM2M, and the conversion of the oneM2M specifications into European Standards

ETSI TC SmartBAN has primary responsibility
- To develop and maintain ETSI Standards, Specifications, Reports, Guides and other deliverables to support the development and implementation of Smart Body Area Network technologies (Wireless BAN, Personal BAN, Personal Networks etc.) in health, wellness, TC SmartBAN’s scope includes communication media, and associated physical layer, network layer, security, QoS and lawful intercept, and also provisions of generic applications and services (e.g. web) for standardisation in the area of Body Network Area technologies.
- To continue activities started by EP eHEALTH to serve as horizontal’ nucleus for the co-ordination of ETSI’s activities in the Health ICT domain (eHEALTH, mHEALTH, pHEALTH etc.) and to co-ordinate ETSI positions on Health ICT related issues including telemedicine and represent ETSI externally. TC SmartBAN scope will not include radio matters (HENs for market access) and EMC.

ETSI ISG CIM developing NGSI-LD standards in ETSI has primary responsibility to
- Develop technical specifications and reports to enable multiple organisations to develop interoperable software implementations of a cross-cutting Context Information Management (CIM) Layer. It is about bridging the gap between abstract standards and concrete implementations.
- Define standard API for cross-cutting Context Information Management enabling close to real-time update/access to information from many different sources (not only IoT).
- Enable applications to register context providers, update context, get actual and historic context information, to subscribe for notifications on context changes, identify appropriate ontologies & data publishing platforms
7. **AIOTI WG03 COOPERATION ON INTEROPERABLE IoT PLATFORMS**

7.1 Introduction

The European Union (EU) aims to create a Digital Single Market source of economic activities and jobs. With the European Commission, the EU supports digital activities with a strategy of research, innovation and standardization in which the Internet of Things plays a crucial role alongside 5G, Big Data, Cloud Computing and Cyber Security.

From 2017, Europe has been recognized as a leader in IoT thanks to the actions of the European Commission. Indeed, the funding of IoT research and innovation projects at different scales (regions, member states, Europe, international collaboration) moving from the stage of experimental IoT platforms to large-scale European pilot projects have for example made it possible to create and recognize the IoT European Alliance (AIOTI) by the IoT alliances, standardization organizations and forums that matter. The next step is to roll out the digital market on a large scale from 2020 with guarantees of safety, security, interoperability, portability, protection of privacy and acceptability of solutions by users.

To achieve ambitious European Digital Single Market and Digitising European Industry goals planned from 2020, technical and societal barriers must be identified and removed.

During the UNIFY-IoT period of 2016-2017, the IoT market was still in its infancy and was rapidly deployed without considering key aspects such as trust in IoT security, privacy (personal data protection, identity protection), interoperability, safety and the freedom to choose and migrate easily between different solutions.

Indeed, there are too many heterogeneous or specialized IoT platforms and not enough portability and interoperability between the different solutions to allow competition. Ideally, only differences in service quality, costs and acceptability (trust) by users should determine the choice of providers. It is therefore expected that IoT services will be delivered through IoT applications and platforms based on interoperable standards at the service level, independently of provider and agnostic to applications in relation to network connectivity solutions. The European regulation on cyber security and the private data protection (and identification data) obliges developers and suppliers of IoT solutions to ensure compliance with the relevant national regulations and European Directives.

IoT solutions must therefore demonstrate this compliance to gain the trust of users and achieve the expected IoT market development.

Of all the existing IoT architectures in all application domains, the lack of recognition of a common IoT reference architecture is a barrier to the interoperability of platforms in each domain and between vertical silos. There are however already IoT reference standards and architectures globally recognized and deployed at the level of radio and service layers. This would be certainly a question of time needed for the demonstration, dissemination and for an adoption by the majority (recognition) of existing open and interoperable solutions alongside dominant global proprietary offers, hopefully, ultimately also adopting these interoperable standards.

Even if the market converges to a common IoT reference architecture (such as AIOTI's HLA / High Level Architecture), based on standards that allow interoperability (at the service and
application level) across silos, it will still be necessary to meet the challenges of security, safety and the protection of personal data across all layers (network, service, application) and through silos / application areas.

Security must ensure resilience of applications, critical data and infrastructure, safety of solutions, and compliance with national and European regulations. A selection of European standards to which IoT applications will have to be able to certify their compliance (in a dynamic process) are the basis of the Cybersecurity Act of September 2017 and the General Data Protection Regulation (GDPR) applicable from May 2018. IoT solutions must be sustainable, efficient and capable of scaling up without loss of quality. IoT solutions must constantly evolve with technical innovations (Blockchain/Distributed Ledger Technologies, Artificial Intelligence, Quantum Computing ...)

In 2016 and 2017 IoT-EPI (and since 2017 the IoT-LSP) proved to the IoT Community how much IERC (EC supported IoT European Research Cluster) plays a catalytic role in Europe. The EC has fostered a collaboration between: IoT Platforms, Large Scale IoT Pilots, AIOTI the Alliance for IoT Innovation (since 2015) and all the H2020 IoT research and innovation projects (since 2008). This coordination of activities is ensured by IERC Task Forces (for IoT Platforms) and Activity Groups (for IoT LSPs), which should lead in 2020 to the deployment of the Large-scale IoT demonstrators that will have lifted the technical and societal barriers identified.

### 7.2 Creation of AIOTI since 2015

The IERC Cluster changed its scope in 2015 and expanded into an informal alliance (initially) named AIOTI (Alliance for Internet of Things Innovation) created under the impetus of the European IoT research community, the European industry and the European Commission. AIOTI (www.aioti.eu) quickly became the flagship of the IoT (IoT Lighthouse) in Europe. IoT interoperability, security, privacy, safety topics were immediately at the heart of AIOTI's work and debates, especially in Europe, which seems to be the most concerned region (even in its regulation on security and privacy - data and identification protection) and the international community expects to get inspired by such recommendations.

It is therefore from the IERC research community, with the support of industrial stakeholders (see https://aioti.eu/members/: ARTEMISIA, Arthur's Legal, ATOS, Bosch, BT, CNH Industrial, Digital Catapult, Engineering LOI, GRADIENT, Huawei, IBM, Infineon Technologies, John Deere, Nokia, Philips Lighting, Samsung, Schneider Electric, Siemens, STMicroelectronics, Telit Communications, and Vodafone), the European Commission and with ETSI support (in WG03) that AIOTI (when the Alliance had an informal structure) has rapidly integrated more than 500 members mainly attracted in the beginning in the following leading working groups:

- WG01 that was “IERC”, chaired by SINTEF
- WG03 "IoT Standardisation" chaired by ETSI
- and WG02 "IoT Innovation" (chaired by Philips Lighting who later became President of the Alliance when AIOTI became an Association).

The IERC was initially (in 2015 and 2016) an integrated Working Group of AIOTI, the WG01 "IERC" (IoT research). In September 2016, when AIOTI formally became a non-profit European Association, IERC has become again the European IoT Research Cluster, close but independent of AIOTI's governance. In February 2018, the legal entity AIOTI contained more than 200 members (a growing number which should reach its maximum of 500 members again, encouraged by a single annual membership fee of only 750 euros per organization). This Alliance is considered by the EC (which is an official observer in the AIOTI statutes) as a European Technology Platform (ETP) developing strategic research and innovation agendas for IoT. In a year and a half (between 2015 and 2016), AIOTI has been officially recognized by the many international players
AIOTI is a reference for the EC in its stakeholder consultations for research programs and regulation in Europe.

Since the creation of the AIOTI, the coordinator of IERC (Ovidiu Vermesan of SINTEF) is also the Chairman of AIOTI WG01 "IoT Research". ETSI (Patrick Guillemin) is the Chairman of WG03 "IoT Standardisation" that also actively maintains formal links with standardization organizations, alliances, fora, research projects and IoT pilots in Europe and worldwide. The organization of the AIOTI Working Groups makes it possible to obtain common solutions (interoperability, security, regulatory compliance, common architecture, etc.) to the different 'silos' (so-called "vertical" application domains) which are now cross connecting thanks to the rapid development and convergence of IoT in all sectors.

### Figure 10: List of 13 Working Groups of AIOTI

<table>
<thead>
<tr>
<th>WG 01</th>
<th>IoT Research</th>
<th>Smart Living Environment for Ageing Well</th>
</tr>
</thead>
<tbody>
<tr>
<td>WG 02</td>
<td>Innovation Ecosystems</td>
<td>Smart Farming and Food Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Weatables</td>
</tr>
<tr>
<td>WG 03</td>
<td>IoT Standardisation</td>
<td>Smart Cities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Smart Mobility</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Smart Water Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Smart Manufacturing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Smart Energy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Smart Buildings and Architecture</td>
</tr>
<tr>
<td>WG 04</td>
<td>IoT Policy</td>
<td>SME interests</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WG 05</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WG 06</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WG 07</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WG 08</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WG 09</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WG 10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WG 11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WG 12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WG 13</td>
</tr>
</tbody>
</table>

Standards Development Organizations (SDOs) already in contact with IERC have strengthened their cooperation with IoT in Europe in AIOTI by participating actively in the work of WG03. The main SDOs initially committed are: 3GPP, oneM2M, ETSI, ITU-T, IEEE, ISO / IEC JTC1, CEN, CENELEC, IETF, W3C as well as fora and consortia such as IIC, OPC-UA and Platform I4.0 etc.

In AIOTI's strategic vision updated in 2017, the first key objective is to be recognized as a major contributor to interoperability, privacy and security and safety of IoT systems and applications around the world, with a focus on creating the necessary trust.

### 7.3 AIOTI work and recommendations

Some simple and pragmatic principles adopted by AIOTI have allowed in less than 2 years to become an open IoT community recognized (and appreciated) by the international IoT community. AIOTI WG03 (IoT Standardisation) does not develop standards but recommendations for standards developing organizations (SDOs), alliances / fora, users and standards influencers (research, innovation, application development and IoT platforms, commercial products and open source project). AIOTI participants feel free to follow and implement these recommendations within their own organizations that develop (or use) IoT standards.
The birth of AIOTI in 2015 has fostered a good collaboration of IoT research (IERC) with innovation and standardization in Europe and worldwide. The challenges identified by AIOTI have made it possible to publish and update a complete IoT landscape, which includes alliances, fora, standardization organizations, research projects and open source projects grouped on the same map for the first time and put in contact (especially within WG03 "IoT Standardisation") to stimulate dialogue, to converge and to work against fragmentation.

The list of the 86 IoT initiatives (SDOs and Alliances / Fora) identified in the IoT landscape maintained by AIOTI WG03 (IoT Landscape V2.8 - June 2017) is:

3GPP (3rd Generation Partnership Project); 5GAA (5G Automotive Association); ACEA (European Automobile manufacturing Association); AEF (Agricultural Industry Electronics Foundation); AIOTI (Alliance for Internet of Things Innovation); Allseen Alliance; ASHRAE; Automation ML; AVNU; Bluetooth; Broadband Forum; Calypso; C2C-CC (Car-2-Car Communication Consortium); CCC (Car Connectivity Consortium); CC-Link; CEN (European Committee for Standardization); CENELEC (European Committee for Electrotechnical Standardization); CIA (CAN IN Automation); CIAlII (China Integration and Innovation Alliance of Internet and Industry); CLEPA; Continua: Health Alliance; Dicom (Digital Imaging and Communications in Medicine); easyway; EEBUS; eCl@ss; ECC (Edge Computing Consortium); ERTICO - ITS Europe; ESMIG; ETSI (European Telecommunications Standards Institute); Enoclean Alliance; GlobalPlatform; GSMA; GS1 (Global Standards 1); HL7 International (Health Level 7); HYPER/CAT; IEC (International Electrotechnical Commission); IEEE (Institute of Electrical and Electronics Engineers); IEEE 802 LAN/MAN Standards Committee; IEEE P2413.; IETF (Internet Engineering Task Force); IHE (Integrating the Healthcare Enterprise); IIC (Industrial Internet Consortium); IPEN (Internet Privacy Engineering Network); IPSO (Internet Protocol for Smart Object); IPv6 Forum; IRTF (Internet Research Task Force); IO-Link; IoT Security Foundation; ISA (International Society of Automation); ISO (International Organization for Standardization); ISO/IEC JTC 1; ITU (International Telecommunication Union); The KNX Association; LoRa Alliance; M2.COM; MIPI Alliance; NB-IoT Forum; NFC Forum; Initiative; OASIS; OAA( Open Automotive Alliance); Open Connectivity Forum; ODVA; OGC (Open Geospatial Consortium); OMA (Open Mobile Alliance); The ULE (Ultra Low Energy) Alliance; OMG (Object Management Group); oneM2M; OPC (Open Platform Communications) Foundation; The Open Group; OSGi Alliance; PI (Profibus - Profinet) International; Platform Industrie 4.0; SAE International; SGIP (Smart Grid Interoperability Panel); Thread group; TMForum; Trusted Computing Group; UDG Alliance; USEF (Universal Smart Energy Framework); W3C (World Wide Web Consortium); Weightless; Wi-Fi Alliance; Wireless World Research Forum; The ZigBee Alliance; XMPP

7.3.2 Common IoT high level architecture (HLA)

Fora/alliance and SDO experts who developed AIOTI's IoT landscape have identified the need to define a common high-level IoT architecture (High Level Architecture / HLA, domain model, functional domain) which made it possible to show the possibility of horizontal convergence of the architectures differences of the so-called vertical domains (silos). For simplicity it turns out that the architectures have the same layers, the same interfaces and the same boxes but do not have the same names. The latest published HLA (Release 3 of June 2017) is maintained by AIOTI and has managed to match (map) the HLA with the main IoT Architectures (oneM2M, 3GPP, ITU-T, ISO / IEC JTC1, IEEE P2413, IIC, NIST, ETSI SmartBAN, W3C, IETF ... Cloud, Edge Computing, Virtualization).
7.3.3 IoT Semantic Interoperability (SemIoP)

7.3.3.1 First AIOTI SemIoP recommendations

The initial work of AIOTI WG03 (with W3C Web of Things, IEEE and oneM2M) confirmed that common and international IoT semantic interoperability (SemIoP) principles can be adopted to lay the technical foundations of existing initiatives that only sought to find a common place (forum) to collaborate, build consensus and solidify their convergent principles. In 2015, the first SemIoP recommendations for H2020-IoT-2016 H2020 IoT LSP (2017-2019 / 2010) projects were endorsed and published by the EC in:


This collaboration led to an acceleration of IoT base ontology standardization in oneM2M (oneM2M TS-0012 version 2.0.0 Release 2) and cartography (mapping) of this ontology in the field of Smart Appliances (Domestic / household appliances) in ETSI TC SmartM2M / SAREF.

7.3.3.2 Second set of AIOTI SemIoP recommendations from the international community

Recognizing that the definition and joint adoption of these first AIOTI SemIoP recommendations [10] should also be adopted by the international IoT community, AIOTI has agreed to let the copyright of contributors to go under "Creative Common" license (https://creativecommons.org/licenses/by/4.0/) and host the first Common SemIoP White Paper under the reseachgate.net portal. This second edition of SemIoP recommendations with AIOTI is in fact the first public and international white paper jointly announced by AIOTI, W3C, oneM2M and IEEE.

7.4 AIOTI recommendations for EU-funded IoT projects

In 2015/2016, before the selection of the H2020 IoT LSPs projects (2017-2020 call H2020-IoT-2016 of 100 Million euros), the AIOTI and IERC community developed and adopted common IoT recommendations published by the EC to tenderers of future H2020 projects, existing IoT global drivers (such as IIC testbeds for example) and H2020 projects (2016-2017) of IoT platforms that were underway (and that formed later IoT-EPI). Since then, these recommendations have been updated and maintained by AIOTI at [10] https://aioti.eu/resources-

The EC (DG GROWTH, DG CONNECT) has funded a Specialist Task Force / STF (STF505) led by ETSI which has published two reports (ETSI TR 103 375 [5] and ETSI TR 103 376 [6]) developed with AIOTI in ETSI TC SmartM2M for the H2020 IoT LSPs pilots being prepared. These reports and recommendations were disseminated in a workshop of the EC in Brussels in February 2017, see https://ec.europa.eu/digital-single-market/en/news/internet-things-platforms-and-standardisation-workshop. All these documents are publicly available and posted on the Internet.

7.5 Summary of IoT-EPI platforms in liaison with AIOTI

Among the many reports produced by IoT-EPI and its Task Forces, a state of the art IoT Platforms (UNIFY-IoT D03.01 "Report on IoT platform activities" [2]) was delivered with some initial key facts:

There were more than 360 IoT platforms identified worldwide by UNIFY-IoT, which are geographically divided as follows: 27% in Europe, 56% in the United States and 11% in Asia and 6% in the rest of the world. (original source - among others - IoT Analytics). The distribution of
the types of platforms is the following: 55% of start-ups, 26% of SMEs, 16% of dominant world corporations (MNC / Multi National Corporations) such as for example Microsoft, IBM, Amazon, Bosch, Cisco, Intel, ARM, etc.

The "MNC" platforms of 4 types are:

**Cloud Centric:**
- Amazon AWS IoT platform, https://aws.amazon.com/iot/

**Industry Centric:**
- GE (General Electric’s) Predix, https://www.predix.io/

**Communications Centric:**
- PTC Axeda, http://www.ptc.com/axeda

**Device Centric:**

Other platforms are

**Small and Medium Enterprises** (SME Small Medium Enterprises),
- ThingsSpeak, https://thingspeak.com
- Xively, https://xively.com/
- Carriots, https://www.carriots.com
- Evrythng, https://evrythng.com
- SensorCloud, https://sensorcloud.com

**Open source platforms:**
- Kaa, http://www.kaa-project.org/
- OpenRemote, http://www.openremote.org/display/HOME/Home
- FIWARE, https://www.fiware.org/:
  Note the collaboration between FIWARE and ETSI ISG CIM, ETSI TC SmartM2M and oneM2M, https://www.fiware.org/2017/01/13/etsi-launches-new-group-on-context-information-management-the-role-of-fiware

UNIFY-IoT’s analysis of IoT platforms shows that the IoT community recognizes the importance of architecture and an interoperable global framework for the oneM2M service layer consisting of:

**Commercial applications:** LG Group (Korea), C-DOT (India), NEC (Japan), Sierra Wireless (Canada), Inter Digital (USA), Qualcomm (USA), KT (Korea), Huawei (China), SK telecom (Korea), Sensinov (France), MODACOM (Korea) and HPE / Hewlett Packard Enterprise (USA)

**Open source** (oneM2M based platforms):
- InterDigital oneMPOWER™, (wot.io™), http://www.interdigital.com/iot
- C-DOT (Center for Development of Telematics, India), http://www.cdot.in
✓ OpenMTC platform, (prototype made by Fraunhofer FOKUS and TU Berlin, used by IoT research projects willing to use oneM2M) http://www.open-mtc.org/
✓ KETI (Korea Electronics Technology Institution) / OCEAN,
✓ Cisco, Open Daylight / IoTDM (Internet of Things Data Management), https://wiki.opendaylight.org/view/IoTDM_Overview

The most referenced Open Source platforms are OpenIoT (4 times), NodeRED (3 times), FIWARE (3 times) with a single Microsoft Azure trading platform (2 times). Of the 35 IoT dominant platforms identified by UNIFY-IoT, 6 of them were referenced by IoT-EPI's 7 RIAs: Bosch IoT SW Suite, Eclipse IoT, Evrythng, Microsoft Azure IoT, Amazon AWS IoT and Eclipse OneM2M.

### 7.6 AIOTI Analysis of IoT Platforms and IoT-EPI

The large number and diversity of IoT platforms selected in 2015 for IoT-EPI projects shows the immaturity and diversity of the offer at this stage of development of the IoT market that corresponds to the launch of AIOTI. In 2015, during the selection of IoT-EPI projects (2016-2017), the EC regretted the absence of proposals highlighting the IoT security and the protection of identification and personal data. This gap still remains a major challenge in 2017 in a time where the regulation has increased its level of requirement with the "Cybersecurity Act" of September 13, 2017 and the GDPR applicable in May 2018. Hopefully in 2018, new security and privacy oriented H2020 RIAs have started (ENACT, SOFIE, IoT Crawler, CHARIOT, SecureIoT, SEMIoTICS, BRAIN-IoT, SerIoT) and results are expected under the monitoring of AIOTI WG03, CREATE-IoT, IoT-LSP (especially Activity Group AG2 and AG5) and ETSI STF 547 (entitled “A coordinated approach for Security/Privacy and (Semantic) Interoperability of standardised IoT Platforms “). STF 547 is including AIOTI Support like STF 505 did with TC SmartM2M.

The year 2017 for IoT-EPI was a pivotal year between the end of the 2016-2017 H2020 experiment of 50 Million Euros of IoT-EPI platforms and the first year of the 2017-2020 H2020 experimentation of 100 million cross-domain IoT Large Scale Pilots (H2020 IoT LSP). The IoT analysis and associated recommendations are therefore evolving and will be further enriched with this experience in Europe and with the work of AIOTI in Europe and internationally.

### 7.7 What’s next for AIOTI?

ETSI coordinates the IERC / IoT LSP Activity Group 2 (AG02) on "IoT standardization, architecture and interoperability" in cooperation with W3C. After 3 to 4 years, before 2020 expectations for CREATE-IoT, IERC, 5 H2020 IoT LSPs and AG02 (+ AG05) will be to produce validation tools on the use of the best selected IoT standards that will allow (standard gap filling) to make IoT applications between domains / silos secure, interoperable and open. AG02 should have been able to manage the redundancies and cover the lack of standards (pre-standardization) identified in the period 2017-2020 period.

IERC's AG02 will also collaborate closely with the IERC AG05 "Trusted IoT, privacy, security and legal frameworks" whose goal is to manage the technological acceptance of IoT, the protection of privacy (protection of personal data), security, safety (vulnerability), responsibility, the needs of users and the potential establishment of an "IoT Trust Label" whose concept was introduced by the EC on September 13, 2017 in the Cybersecurity Act.
The IoT community awaits a lot of work and collaboration between the EC, IERC, IoT-EPI, IoT-LSP and AIOTI, it will follow the publications (freely available) of AIOTI and the communications / regulations of the EC in the hinge period 2017-2020.

In the short term (2020's) regarding the future of the Internet of Things, despite the significant threats and challenges that are posed today, there is enough to be confident in the capacity and the means of the IoT community.

All the collaborating stakeholders:
• The European Commission,
• European researchers (IERC),
• Public and private pilots coordinating and cooperating with
  • Standardization bodies,
  • Alliances, consortia around the world,
  • Developers, operations managers,
  • Users, SMEs, innovative actors,
• Open source projects will offer more
  • Interoperable, open,
  • Secure,
• Compliant IoT applications in line with European regulations,
• Security standards, data protection standards and privacy rules that will give confidence in the Internet of Things that will become part of our daily lives.

IoT market maturation work will also include **new and emerging technology** trends: 5G offering Internet responsiveness of 'real-time' information systems (Tactile Internet), Blockchain, Quantum Safe Cryptography / QSC, Artificial Intelligence / AI, Virtualization of IoT operating systems for agile Cloud / BigData (Open IoT Platform as a Service) agile deployments, autonomous robotic vehicles and systems, integration of mixed physical and virtual cyber systems (such as augmented reality) with more autonomy, self-learning and AI.

Quantum Computing (combined with AI) appear to be a key trend to monitor for IoT. Since there are already real quantum computer prototypes (those of IBM, Google, Intel and Microsoft) and quantum computer simulators (Quantum Learning Machine / QLM by Atos) and physical systems (products) based on quantum physics (Random Number Generator, Quantum Key Distribution / QKD), it is possible that by 2030 (or before) quantum computation and cryptography will bring us into a new age of ICT.
8. CHALLENGES, ISSUES AND GAPS

8.1 Impact of IoT standards on interoperability and platforms
Some of the recent approaches addressed in the present document are outlining a dual movement in the approach of the development of IoT systems. One the one hand, IoT systems are facing very complex and pressing requirements (e.g., number of components; volume of data; latency or reliability; security; privacy) that tend to drastically increase their complexity. On the other hand, some new approaches are emerging and are being validated (e.g., layered architectures; new interoperability frameworks; marketplaces; semantic interoperability; virtualisation) that are likely to reduce systems complexity; to provide more flexible applications development; and to open the development of systems to a larger number of stakeholders with new value propositions.

This evolution comes with a number of challenges regarding the current approach to the developers of IoT systems and more generally to the IoT community. Some of the following issues that will have to be tackled are addressed in his section.

8.1.1 Design and deployment of IoT Systems

8.1.1.1 Open and efficient implementations.
Openness is a clear requirement of the IoT technical community. Most of the platforms described above are based around a combination of layers, interoperability solutions, APIs, etc. that grant the possibility of assembling the most appropriate solution for every part of the IoT system in a flexible manner. In order to ensure that these expected benefits will materialize, open and flexible architectures will have to be supported by a large catalogue of effective, easily available and possibly certified components available through marketplaces. A growing number of these components will be provided by the Open Source Software (OSS) and the mechanisms for a seamless integration have to be developed, implemented and validated.

Emerging development techniques must support the development of fine-grained components that interact with a plurality of others. In the case of existing IoT systems, their introduction may require that some currently used solutions (applications, building blocks) be split in smaller (interacting) units. The platforms will have to adapt to this and not all of the currently in use may be fit for the transformation.

Finally, most of the new IoT systems will have to be extremely effective from a number of non-functional properties such as latency, reliability, near real-time handling of massive quantities of data, etc. The introduction of techniques such as Cloud or Edge computing, microservices-based architectures are expected to answer this kind of requirements. The support of IoT platforms and standards will be required.

8.1.1.2 Integration with legacy
Only a limited number of IoT systems can be fully seen as greenfield, built from scratch. Most of them have (or will have) to incorporate existing (and sometimes long existing) elements. The introduction of all the new techniques discussed above (in section 3) may not be possible for the entire system, possibly for cost reasons and possibly because of difficulties related to old or unmaintained technologies. The potential coexistence of old and new parts (the latter based on those new approaches, e.g., interoperability patterns or semantic interoperability) will require some adaptations.
8.1.3 Federation

The question of federation of systems is much debated in the IoT community, in particular by the Research community, and somehow by the Standard community. The need for federation of IoT systems is becoming a credible requirement for some Use Cases like Smart Cities (and even in Industrial IoT). To a large extent, beyond the identification of significant use cases, the question of efficient solutions is key. From this standpoint, approaches such as interoperability patterns or marketplaces may be and will have to be validated (using, in particular, the experience of the IoT-EPI projects).

8.1.2 Privacy and data confidentiality

Privacy is universally pointed out as a key enabler for trusted IoT systems. It has long been considered as the "poor cousin" in the industry, until a repeated number of failures due to the non-acceptance of systems for privacy reasons has brought the issue on top of the requirements list. In addition to this, the advent and staring deployment of General Data Protection Regulation (GDPR) has become an important motivating factor for the (IoT) community to embrace the issue.

GDPR forces a reconsideration of the current approaches for personal data (and identification) protection and related security. From a process-centric approach, the systems supporting GDPR must switch to a more user-centric and data-centric approach. This will have an impact on the security technology embedded in architectures and platforms. Overall, the current security standards framework will be impacted and a new breed of standards will have to emerge (some already on the workbench).

8.1.3 Security

Just as Privacy, Security is a key enabler for trusted IoT systems. From this standpoint, there is no silver-bullet solution for security in the current (IoT) systems. The current approach in most of the IoT platforms is to provide a (standards-based) support for solutions at each layer of the IoT system HLA, (e.g., in order to support authentication and authorisation). But, ensuring global, cross-layer security (as depicted in Figure 5) is still a complex task and the emerging techniques in support of IoT systems interoperability largely continue to rely on the assumption that the provision of security at each layer if the HLA is, in most cases, sufficient.

In addition to the integrity of the system, Security has also a key role to play as a support to Privacy. As pointed out in [17]: "There is no data protection without security. This goes for both personal data as well as any non-personal data. For instance, personal data protection and privacy is as much about security as it is about data management. Through IoT products, systems and services, organizations create, collect, process, derive, archive and (ideally and to the extent permitted) delete large amounts of data.". This is creating an additional level of requirements on security solutions and on the underlying standards support. The user and data centric approach mentioned in section 8.1.2 is a promising way forward.

8.1.4 Regulation.

Regulation is, for the most part, not the premier subject of attention and concern for systems and applications designers and developers, and this is also true for IoT. However, it is expected that it will play a more significant role in these systems in the short-term. The obvious example of the (GDPR) about to be fully deployed in Europe is one obvious example.

Other aspects of regulation may not be currently fully apparent but may become significant. As an example, the general trend towards more virtualisation (i.e. massive use of Cloud Computing techniques and solutions) in IoT systems will introduce new requirements on the systems which may have a regulatory dimension. For instance, virtualisation will introduce more consideration
of the role of Cloud Service Providers or of business-related issues such as Service Level Agreements (SLA). Even if general of IoT-specific standardisation is working on these issues, their regulatory dimension may become a subject of concern.

8.2 Gaps
The identification and resolution of gaps is a clear concern for the IoT community. These gaps are not just related to missing technologies and types of gaps can be perceived and not to be identified and addressed as well. In the ETSI Technical Report on IoT Gaps (see [6]), three categories of gaps have been addressed:
- "Technology gaps with examples such as communications paradigms, data models or ontologies, or software availability.
- Societal gaps with examples such as privacy, energy consumption, or ease of use.
- Business gaps with examples such as silo-ed applications, incomplete value chains, or missing investment."

Once the gaps have been identified, the actors in the technical community (standardisation in particular) may perceived differently the criticality depending on the role. Some of the gaps identified in the ETSI report above have been evaluated by the European IoT Large-Scale Pilots (LSPs). The Table 3 below is listing these gaps and provides an average view of their criticality coming from the LSPs evaluation. The criticality could be different with other actors (e.g., users, service providers).

<table>
<thead>
<tr>
<th>Nature of the gap</th>
<th>Type</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Competing communications and networking technologies</td>
<td>Technical</td>
<td>Medium</td>
</tr>
<tr>
<td>Easy standard translation mechanisms for data interoperability</td>
<td>Technical</td>
<td>Medium</td>
</tr>
<tr>
<td>Standards to interpret the sensor data in an identical manner across heterogeneous platforms</td>
<td>Technical</td>
<td>High</td>
</tr>
<tr>
<td>APIs to support application portability among devices/terminals</td>
<td>Technical</td>
<td>Medium</td>
</tr>
<tr>
<td>Fragmentation due to competitive platforms</td>
<td>Business</td>
<td>Medium</td>
</tr>
<tr>
<td>Tools to enable ease of installation, configuration, maintenance, operation of devices, technologies, and platforms</td>
<td>Technical</td>
<td>High</td>
</tr>
<tr>
<td>Easy accessibility and usage to a large non-technical public</td>
<td>Societal</td>
<td>High</td>
</tr>
<tr>
<td>Standardized methods to distribute software components to devices across a network</td>
<td>Technical</td>
<td>Medium</td>
</tr>
<tr>
<td>Unified model/tools for deployment and management of large scale distributed networks of devices</td>
<td>Technical</td>
<td>Medium</td>
</tr>
<tr>
<td>Global reference for unique and secured naming mechanisms</td>
<td>Technical</td>
<td>Medium</td>
</tr>
<tr>
<td>Multiplicity of IoT HLAs, platforms and discovery mechanisms</td>
<td>Technical</td>
<td>Medium</td>
</tr>
<tr>
<td>Certification mechanisms defining “classes of devices”</td>
<td>Technical</td>
<td>Medium</td>
</tr>
<tr>
<td>Data rights management (ownership, storage, sharing, selling, etc.)</td>
<td>Technical</td>
<td>Medium</td>
</tr>
<tr>
<td>Risk Management Framework and Methodology</td>
<td>Societal</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Table 3: Perceived criticality of some Standards Gaps (Source: CREATE-IoT)

The characterization of gaps is a work-in-progress in the IoT Standardisation community, in particular for the SDOs/SSOs. The mapping of identified gaps on the AIOTI-based architectural framework (described in section 3.2) is a useful reference.
8.3 Standards in support of interoperability in IoT

Interoperability will be an essential element in order to ensure seamless communication and seamless flow of data across sectors and value chains in the coming IoT systems. The emergence of the new approaches to interoperability addressed in the current document will have an impact on the work program of IoT standardisation which is, by nature, not predictable.

However, some trends will have to be taken into account in order to ensure that new standards developments will foster collaboration and reduce fragmentation:

- Solutions should promote “horizontal” standards rather than “vertical” specific ones;
- Interoperability solutions should seek for the integration into “horizontal” frameworks (e.g., oneM2M) supported by open platforms;
- Address cross-layer solutions (e.g. data management, security) must be also supported by standards; and provided by the SDOs and SSOs;
- Effective security and privacy solutions are key to user acceptance and should be based on global holistic approaches (e.g., security by design, privacy by design, user-centric and data-centric solutions);

Some new trends in the design of IoT systems (e.g., IoT virtualisation) will be supported by a massive reuse of OSS components. This is challenging the traditional role of standards. On the other hand, the new approaches to the design of IoT systems may also require that some existing building blocks (and associated standards) be re-considered and in turn promote the development of new standards.
9. REFERENCES

[16] "An Introduction to Internet of Things (IoT) and Lifecycle Management: Maximizing Boundaryless Information Flow™ through Whole-of-Life Lifecycle Management Across IoT", The Open Group, https://www2.opengroup.org/ogsys/catalog/W167
10. APPENDICES AS PUBLISHED BY IoT EPI TASK FORCE

10.1 The IoT-EPI Platforms

10.1.1 Platforms in the AGILE project

AGILE builds a modular hardware and software gateway focusing on the physical, network communication, processing, storage and application layers. The AGILE software modules are addressing functions such as device management, communication networks like area and sensor networks and solution for distributed storage. It considers all the modules needed to provide a robust security management solution.

<table>
<thead>
<tr>
<th>IoT platform</th>
<th>Nature of platform</th>
<th>Brief description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resin.io</td>
<td>Commercial</td>
<td>Device management platform for Linux based IoT devices. It makes it simple to deploy, update, and maintain code running on remote devices.</td>
</tr>
<tr>
<td>Eclipse IoT</td>
<td>Open source</td>
<td>Eclipse smart home, an IoT platform for smart home environments and Eclipse Kura an OSGI based framework for IoT gateways.</td>
</tr>
<tr>
<td>NodeRED</td>
<td>Open source</td>
<td>Tool for wiring together hardware devices, APIs and online services in new and interesting way. Visual IoT service enablement platform developed by IBM.</td>
</tr>
</tbody>
</table>

Table 4: AGILE platforms

10.1.2 Platforms in the bIoTope project

bIoTope provides an architecture for the use of open standards and recommendations for use case implementations that enable stakeholders to easily create new IoT systems and services by using an advanced Systems-of-Systems (SoS) capabilities. It also develops and provides standardised open APIs to enable interoperability and addresses all the layers of the IoT architecture in a cross-domain environment.

<table>
<thead>
<tr>
<th>IoT platform</th>
<th>Nature of platform</th>
<th>Brief description</th>
</tr>
</thead>
<tbody>
<tr>
<td>O-MI/O-DF Reference Implementation</td>
<td>Open source</td>
<td>Implementation of O-MI and O-DF standards for the IoT that makes it easy to set up standard-based IoT node instances. Mainly used for “sandbox” installations but can be scaled up for “industry-level” purposes.</td>
</tr>
<tr>
<td>DIALOG</td>
<td>Open source</td>
<td>IoT Middleware originally developed by Aalto in 2001, which has been further developed and used in numerous research projects as well as industrial pilots.</td>
</tr>
<tr>
<td>NodeRED</td>
<td>Open source</td>
<td>Tool for wiring together hardware devices, APIs and online services in new and interesting way. Visual IoT service enablement platform developed by IBM.</td>
</tr>
<tr>
<td>Warp 10</td>
<td>Open source</td>
<td>Platform for storage, management and analysis of IoT data, especially for Geo Time Series.</td>
</tr>
</tbody>
</table>
| FIWARE       | Open source        | FIWARE is a middleware platform for the development and global deployment of applications for Future Internet. It is an
outcome of a large investment of the EU into large-scale research programme involving network vendors and operators.

Open IoT
- Open source
- OpenIoT is a sensor middleware platform that eases the collection of data from heterogeneous sensors, while ensuring their semantic annotations. It enables semantic interoperability in the cloud and provides IoT app development tools.

Mist
- Closed-source
- Software stack for distributed, secure IoT deployments of ControlThings.

eAir web
- Closed-source
- Cloud service for remote use and management of Enervent Air Handling units.

Other
- Open/Closed source
- Numerous platforms such as BMW’s platform, several Smart Parking platforms in Helsinki, OpenDataSoft’s platform. Estimated over 10 different platforms used now or in the future.

Table 5: BiTope platforms

10.1.3 Platforms in the BIG-IoT project

BIG IoT develops a generic, unified Web API for IoT platforms. As part of BIG IoT, 8 partner IoT platforms are being integrated. BIG IoT focusses on the upper layers of the IoT architecture by addressing the security management, APIs, service integration, external system services, applications, and the business enterprise.

<table>
<thead>
<tr>
<th>IoT platform</th>
<th>Nature of platform</th>
<th>Brief description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Data Platform</td>
<td>Open source</td>
<td>CSI Piemonte’s Smart Data Platform (SDP) is a self-service platform enabling application development based on Internet of Things and Big Data. SDP is based on project Yucca which allows for interconnecting applications, social networks, systems and distributed objects and collecting data and information, by processing and analysing them to develop end-to-end solutions</td>
</tr>
<tr>
<td>Smart City Platform</td>
<td>Commercial, Bosch</td>
<td>Considering solutions for Smart Cities, the requirements differ from those known for classical enterprise applications. In fact, Smart City installations are composed of many different solutions individually customized for the city, but with a common need w.r.t. operation, data sharing and security. The Smart City platform (SCP) targets to connect the silos in the Smart City, i.e., governance, mobility, energy, environment, industry life, tourism, etc. Bosch SCP offers tools and methods to develop, operate and maintain such systems without sacrificing data security and privacy.</td>
</tr>
<tr>
<td>Wubby Platform</td>
<td>Commercial, Econais</td>
<td>Wubby is an ecosystem of software components and services for rapid development of everyday objects. Everyday objects are physical objects embedded with electronics, software, sensors and network connectivity to collect and exchange data.</td>
</tr>
<tr>
<td>OpenIoT Platform</td>
<td>Open Source</td>
<td>OpenIoT is a sensor middleware platform that eases the collection of data from heterogeneous sensors, while ensuring their semantic annotations. It enables semantic interoperability in the cloud and provides IoT app development tools.</td>
</tr>
<tr>
<td>Traffic Information</td>
<td>Commercial, VMZ</td>
<td>The TIC mobility platform provided by VMZ is a data and service platform that has been developed to provide comprehensive</td>
</tr>
</tbody>
</table>
information on all mobility options available in Berlin. The platform includes real-time data from the traffic information center, mobility operators and infrastructure providers and provides a multimodal routing platform using the modal router offered by third parties.

**Bitcarrier/ Sensefield/ FastPrk**

Commercial, World Sensing

Worldsensing provides a unique traffic management portfolio for Smart Cities that includes Bitcarrier, a real-time intelligent traffic management and information solution designed for both road and urban environments. Fastprk provides an intelligent parking system and Sensefields provides an innovative system for detecting and monitoring vehicles and traffic flow.

**BEZIRK Platform**

Open Source

Bosch’s Bezirk platform is a peer-to-peer IoT middleware for both communication and service execution on local devices following the service-oriented paradigm. Bezirk is developed with a view to facilitate asynchronous interactions between the different components of an application with respect to distribution across different devices in a network.

### Table 6: BIG IoT platforms

<table>
<thead>
<tr>
<th>IoT platform</th>
<th>Nature of platform</th>
<th>Brief description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEAMS</td>
<td>Proprietary, EU project</td>
<td>Smart, Energy-Efficient and Adaptive Management Platform (SEAMS) is a state-of-the-art prototype-monitoring tool developed and implemented within the framework of the European project SEA TERMINALS at Noatum Container Terminal Valencia. The SEAMS platform prototype is capable of monitoring the machines and equipment that are being used at a Port Container Terminal.</td>
</tr>
<tr>
<td>I3WSN</td>
<td>Academic platform</td>
<td>Industrial Intelligent Wireless Sensor Networks for indoor environments, platform developed by Universitat Politècnica de Valencia.</td>
</tr>
<tr>
<td>e-Care Tilab Platform</td>
<td>Proprietary</td>
<td>Mobile Health Platform developed by TI, and connecting IoT devices used to monitor patients and the cloud.</td>
</tr>
<tr>
<td>Unical BodyCloud</td>
<td>Open source</td>
<td>BodyCloud is an open platform for the integration of BSNs with a Cloud Platform-as-a-Service (PaaS) infrastructure and it’s currently based on Google App Engine.</td>
</tr>
<tr>
<td>NodeRED</td>
<td>Open source</td>
<td>Tool for wiring together hardware devices, APIs and online services in new and interesting way. We will use it in the AS2AS interoperability framework.</td>
</tr>
<tr>
<td>OpenIoT</td>
<td>Open source</td>
<td>OpenIoT is a sensor middleware platform that eases the collection of data from heterogeneous sensors, while ensuring their semantic</td>
</tr>
</tbody>
</table>
Public annotations. It enables semantic interoperability in the cloud and provides IoT app development tools.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Nature of platform</th>
<th>Brief description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIWARE</td>
<td>Open source</td>
<td>FIWARE is a middleware platform for the development and global deployment of applications for Future Internet. It is an outcome of a large investment of the EU into large-scale research programme involving network vendors and operators.</td>
</tr>
<tr>
<td>UniversAAL</td>
<td>Open Source</td>
<td>UniversAAL is an IoT platform developed in the framework of an FP7 project and applied currently in different AAL, eHealth and AHA environments.</td>
</tr>
<tr>
<td>Eclipse OM2M</td>
<td>Open Source</td>
<td>Open source project based on oneM2M started by LAAS-CNRS and currently under Eclipse umbrella</td>
</tr>
<tr>
<td>Microsoft Azure IoT Suite</td>
<td>Proprietary Microsoft</td>
<td>Provides an easy to configure back-end for IoT deployments. It provides data collection, in-motion analysis, storage and visualization. Complete REST API and provides strong security mechanisms. Domain agnostics, provides no models for data.</td>
</tr>
<tr>
<td>Amazon AWS IoT</td>
<td>Proprietary Amazon</td>
<td>AWS module specially intended to IoT systems. It enables a straightforward access to Amazon Cloud thanks to a easy to use management interface and a REST API to control the status of the things connected. Once data is sent to the AWS IoT, then it can be used the huge ecosystem of AWS cloud solutions. This platform is completely domain agnostic and provides a strong security protection.</td>
</tr>
</tbody>
</table>

Table 7: Inter IoT platforms

10.1.5 Platforms in the symbIoTe project

symbIoTe is providing an abstraction layer for a unified view on various IoT platforms and sensing/actuating resources. In the application domain, a high-level API for managing virtual IoT environments is offered to support cross-platform discovery and management of resources, data acquisition and actuation as well as resource optimization. symbIoTe focuses on seven layers of the IoT architecture from physical to application layer and considering the full security management suite.

<table>
<thead>
<tr>
<th>IoT platform</th>
<th>Nature of platform</th>
<th>Brief description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenIoT</td>
<td>Open source</td>
<td>OpenIoT is a sensor middleware platform that eases the collection of data from heterogeneous sensors, while ensuring their semantic annotations. It enables semantic interoperability in the cloud and provides IoT app development tools.</td>
</tr>
<tr>
<td>Symphony</td>
<td>Commercial, Networks</td>
<td>Networks platform for the integration of home and building control systems. Symphony can monitor, supervise and control many different building systems, devices, controllers and networks available from third-party suppliers. It is a service-oriented middleware, able to integrate several functional subsystems into a unified IP based platform.</td>
</tr>
<tr>
<td>Mobility Back-end as a Service (MoBaaS)</td>
<td>Commercial, Ubiwhere</td>
<td>System integration platform to wrap around different city data sources. Application enablement environment geared towards smart city apps focusing on transport and mobility aspects of cities.</td>
</tr>
</tbody>
</table>
A software platform designed and conceived to allow agile, continuous management of data in the fields of energy efficiency, security and automation. Cloud-based communication software that enables clients to easily and intelligently connect machines and devices to the cloud and then process, transform, organize and store machine and sensor data.

A vertical IoT platform created to manage digital assets pertaining to harbours used for boating and yachting. Its focus is to provide services to the harbour’s activities (B2B) and to its end-users (B2C).

A mobile health data collection and online therapy management system. It integrates different sensor devices on the client side and provides backend interfaces for health management systems.

Table 8: symbIoTe platforms

10.1.6 Platforms in the TagItSmart project

TagItSmart offers a set of tools and technologies integrated into a platform with open interfaces enabling users across the value chain. The project address seven layers of the IoT architecture working on modules for security management, business logic, service integration, storage, APIs, big data analytics and business enterprise.

Table 9: TagItSmart platforms

10.1.7 Platforms in the VICINITY project

The VICINITY project focuses on a platform and ecosystem that provides “interoperability as a service” for infrastructures in the IoT and addresses the five-upper layer of the IoT architecture. The work considers the service integration, business logic, virtualisation, storage, APIs, tools, external system services, applications, data analytics and cloud services.
### Vicinity

<table>
<thead>
<tr>
<th>IoT platform</th>
<th>Nature of platform</th>
<th>Brief description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LinkSmart</td>
<td>Open source</td>
<td>IoT middleware originally developed in the Hydra project. It allows developers to incorporate heterogeneous physical devices into their applications through easy-to-use web services for controlling any device.</td>
</tr>
<tr>
<td>IoTivity</td>
<td>Open Source</td>
<td>IoTivity is an open source software framework enabling seamless device-to-device connectivity to address the emerging needs of the Internet of Things.</td>
</tr>
</tbody>
</table>

Table 10: Vicinity platforms