**DEI WG2 Questions and Answers (provided by AIOTI WG03 members)**

**Editor: Georgios Karagiannis (AIOTI WG03 vice-chair)**

**Question 1: What is the current landscape of IoT activities in Europe (national initiatives, EU funded activities, other)?**

**Individual answers from AIOTI WG03 members (not necessarily representing opinion(s) of the company/organisation that the AIOTI WG03 member is working for):**

**Answer to Question 1 provided by Juergen Heiles (**[**juergen.heiles@siemens.com**](mailto:juergen.heiles@siemens.com)**)**

<JH>: From WG03 we can provide our landscape document as an input. We may filter it for European activities. The question is what does European activities mean, only standardization activities in ETSI, CEN ,CENELEC, AIOTI, national bodies, .. or also the involvement of European companies in international activities?

**Answer to Question 1 provided by Omar Elloumi (omar.elloumi@nokia.com)**

OE> I agree, the question is too vague. But here is my quick attempt. The landscape of IoT activities in Europe is mainly composed of:

* Research and innovation related activities either privately funded or as part of collaborative projects
* Standards: while those standards may have EU roots, they often contribute to international standards or are globally applicable. The ESO (European Standards Organizations) play an important role when it comes to supporting policy actions such as EC mandates or regulation.
* Industry associations which are based on partnerships between, mostly, industry players. They serve the need of creating favorable industry environment to influence standards, conduct experimentation (at large scale), provide project management expertise supporting R&I projects, etc..
* Different industry players (SMEs, large manufacturers, service providers, system integrators, device manufacturers, etc) building/operating products and services for IoT domains such as automotive, smart cities, etc.

**Answer to Question 1 provided by Emmanuel Darmois (for STF 505)**

The landscape of IoT Standardization as it is detailed in the STF 505 report (ETSI Technical Report TR 103 375) is large and apparently fragmented. There is a relatively large number of standards involved: 329 standards, of which 150 are generic (i.e. apply across several vertical domains) and the 179 others apply to specific verticals. Though it seems a rather high figure, the spread of scope of these standards is also large, with an important result: on a specific domain, there are – in general, with a few exceptions, such as in wireless access - not so many competing standards. So, though it is correct to say that the landscape is fragmented, this is especially true for some specific (though quite significant) domains.

It should be noted that the IoT standards identified are very often – at least for the generic ones - related to communications. This is largely reflecting the importance of standards at the overall "platform" (in the sense of platforms such as oneM2M) level. When interoperability is at stake, standards are really needed and, in general, there are available.

However, many existing standards are also related to the exchange of information within and between systems. There is quite a number of existing Information Models that are used – for the large part – within vertical domains. The approach of semantic interoperability that is meant to increase the flexibility and dynamicity of these models is not yet very visible at standards level (with some exceptions such as SAREF).

**Answer to Question 1 provided by Davide Brandano (davide.brandano@APPLUS.COM)**

DB: In Spain there are some relevant initiatives and Pilots: some of them are currently in progress, some other ones are already finished and further other ones are planned in the near features.  What is very interesting is that such initiatives and Pilots are involving different technologies of LPWAN (both over cellular and unlicensed sub-GHz spectrum) for different applications / uses cases. Following the most relevant ones that are already notified through several advertising channels, publically available:

1. NB-IoT Pilot on Live Network for Smart Parking in Spain
   1. Involving Vodafone, Huawei, Fangle, Ublox
   2. the trial took place in Vodafone Plaza in Madrid and covered various indoor parking spots. Smart Parking will allow users to access parking data remotely from mobile application, including checking parking spot availability, navigating to the available spots, etc. In addition, the solution will create new revenue streams for the municipal management, lower public parking running costs as well as help to alleviate traffic congestion. The trial will be turned into a live demonstration inside the Business Exhibition Centre at the plaza to showcase the solution to Vodafone’s customers and visitors.
   3. More info: <http://www.huawei.com/en/news/2016/6/NB-IoT-industry-partners-for-Smart-Parking-pilots>
2. NB-IoT Pilot on Live Network for Smart Metering in Spain
   1. Involving Vodafone, Huawei, Ublox, “Aguas de Valencia” (a Service Provider for Water management)
   2. The pilot test has demonstrated the feasibility of this technology (NB-IoT) and it was carried out in the Valencian municipality of Moncada, managed by Grupo “Aguas de Valencia”, where narrowband cellular devices over LTE (according Rel. 13 3GPP Standardization) were placed in difficult access facilities where optimum data transfer is a challenge. The success of this Pilot will will allow in the future a massive deployment of smart meters, in a simpler, faster and more efficient way, both in the more than 300 national and international supplies managed by the Aguas Group. Vodafone Spain has been responsible for integrating the technology in the mobile network and, therefore, the Aguas de Valencia Group, in its interest to continue improving the communications of the smart meters and to achieve the transmission of data without infrastructures, opted to take to carried out a pilot project at its Moncada facility.
   3. More info: <http://www.gsma.com/connectedliving/wp-content/uploads/2015/12/Presentation-3_Vodafone-keynote-v5.pdf>
      1. For the mentioned Pilots, see slide 8
      2. Here other initiatives are highlighted
3. Smart Cities in Catalonia (updated 15/11/2016)
   1. 270 Companies involved (82% are SMEs), 36.650 M€ revenue, 116.163 employers involved (2015)
   2. 6.969 M€ of revenues only related to Smart City activities (2015), which represents the 3% of the Catalan GDP
   3. Barcelona is the city of Catalonia where the 84% of those Companies are located
   4. 51% of the such  Companies are for Export services, 17% having foreign presence also.
   5. Barcelona is the second smart city of the world, after Singapore (according *Juniper Research, 2016*)
   6. The sectors with the bigger critical mass are:
      1. Waste management
      2. Smart Mobility
      3. Smart Lighting
   7. Most of the services over unlicensed sub-GHz band
   8. More info: <http://coneixement.accio.gencat.cat/c/document_library/get_file?uuid=a1d6c560-a159-4035-9837-cdde922186ea&groupId=30582>
   9. Smart  Project/Pilots in Catalonia
      1. 67 between Projects and Pilots planned, Implemented, running and finalized
         1. Areas
            1. Citizens
            2. Commerce
            3. Culture
            4. Energy
            5. Education
            6. Governance
            7. Urban ICT infrastructure
            8. Innovation and economic development
            9. Environment
            10. Mobility
            11. Resiliency and security
            12. Healthcare and social services
            13. Urban services
            14. Tourism
            15. Urbanism

More info: <http://observatorismart.cat/>

**Answer to Question 1 provided by Georgios Karagiannis (**[**georgios.karagiannis@huawei.com**](mailto:georgios.karagiannis@huawei.com)**) – AIOTI WG03 vice-chair**

Georgios: The AIOTI WG03 (IoT Standardisation) identifies and, where appropriate, makes recommendations to address existing IoT standards and analyses gaps in standardisation, and develops strategies and use cases aiming for (1) consolidation of architectural frameworks, reference architectures, and architectural styles in the IoT space, (2) (semantic) interoperability, (3) security and (4) personal data & personal data protection to the various categories of stakeholders in the IoT space.

AIOTI WG03 published several deliverables, one of them is denoted as “IoT LSP Standard Framework Concepts”, and can be downloaded via: <https://docbox.etsi.org/SmartM2M/Open/AIOTI/!!20160530Deliverables/AIOTI%20WG3_sdos_alliances_landscape_-_iot_lsp_standard_framework_concepts_-_release_2_v6.pdf>

This deliverable introduces IoT Standards Developing Organisation (SDO), Alliance and Open Source Software (OSS) landscapes. The main objective of this deliverable is to briefly present the global dynamics and landscapes of IoT SDO, Alliance and OSS initiatives, which can be used among other (1) to leverage on existing IoT standardization, industry promotion and implementation of standards and protocols, 2) as input for LSP (Large Scale Pilot) standards framework and gap analysis and 3) to provide a guideline for the proponents of future project proposals associated with future IoT related calls financed by the EC on the positioning of these initiatives within these landscapes.

The realization of the IoT evolution and remaining challenges involve the development of standards and protocols and as well the industry promotion and implementation of these standards and protocols. This depends severely on the work and activities accomplished in SDO (Standards Developing Organization), Alliance and OSS (Open Source Software) initiatives. It is therefore, important to understand the global dynamics and landscapes of IoT SDO, Alliance and OSS initiatives.

Currently there are many SDO, Alliance and Open Source initiatives that are active and competing in the IoT technology and applications areas. This is a normal development considering that IoT technology is still in the early phase of deployment. In this context, the landscape is complex, dynamic and challenging to grasp and visualize.

This report gives several ways of visualising the landscape in order to simplify and facilitate the usage of the information in various IoT application domains. AIOTI WG03 has chosen three ways for this representation. First, the IoT landscape is divided into four quadrants, where the horizontal axis represents the market type and the vertical axis represents the technology area covered by these initiatives; second the initiatives are classified based on the vertical and horizontal application domains and third the IoT landscape initiatives are clustered on seven knowledge areas (e.g. sensors/actuators/edge devices, communication/connectivity, integration/interoperability, applications, architecture, and security/privacy).

One example of this visualization that is taken from this AIOTI WG03 report is shown in the below figure. This figure shows the “IoT SDOs and Alliances Landscape (Technology and Marketing Dimensions)”, where these initiatives are projected based on two projection dimensions. The horizontal axis represents the market type and the vertical axis represents the technology/solution/knowledge area that these initiatives cover and focus. It should be understood that the most left part of the horizontal axis represents the customer (i.e., Business to Customer: B2C) market, while the most right part of the same axis represents the industrial internet (i.e., Business to Business: B2B) market. The top part of the vertical axis represents the technology areas that are related to services and applications, while the bottom part of the same axis represents the technology areas that are related to connectivity.

From the point of view of IoT platforms a detailed overview is provided in the report that is published by the Unify IoT project” ICT-30-2015: Internet of Things and Platforms for Connected Smart Objects” published a Report on IoT platform activities that can be retrieved via::

<https://docbox.etsi.org/SmartM2M/Open/AIOTI/IoTPlatformsAnalysisToImprove/D03_01_WP03_H2020_UNIFY-IoT_Final.pdf>

AIOTI WG03 will use this report and will elaborate on the derived conclusions from this report.

Some conclusions from this report are as follows.

The IoT Platform market represents a new dynamic segment that emerged few years ago, and as in any new markets, the landscape is complex and changing very rapidly. The immaturity of the current IoT platform market is evident due to the sheer number of providers actively offering solutions. This oversaturation of IoT platforms on the market will lead to consolidation and many platforms going out of business in near future. Increasing standardisation and joint efforts in open source development across major players will see a more aligned landscape emerging.

**Answer to Question 1 provided by Valentijn de Leeuw (Gérant) [mailto:Valentijn@kyoyu-sha.eu]**

<VVdL> I think we could look if de facto open source platforms with common services layers capable of building IoT applications, such as Cloud-foundry, are capable of cross-industry applications suitable for Europe’s LSP’s, and in line with the IoT-Architecture and similar standard.  If not we should look at evolving Cloud-foundry or similar to make it suitable.

**Answer to Question 1 provided by Harris Moysiadis [mailto:tmoysiadis@f-in.gr]**

HM: There are many differences on the national adoption rates of IoT technologies including the available funds for local deployments, umbrella organizations, PPPs that each Member State has allocated to. The Innovators of the area shall transfer their know-how to the relevant stakeholders ensuring smooth coordination among national initiatives, EU initiatives and EU SDO progress. All these have to contribute to the DSM vision.

**Answer to Question 1 (IoT Semantic Interoperability) provided by Aitor Corchero Rodriguez (**[**aitor.corchero@EURECAT.ORG**](mailto:aitor.corchero@EURECAT.ORG)**)**

The "IoT Semantic Interoperability" is a transversal topic that is continuously being considered in H2020 project/proposals and associations. Accordingly, the activities related to this topic is considered in:

* **IoT Schema.org (international):** Focused on semantic interoperability in Smart Homes (mainly).
* **Open geospatial Consortium (international):** Aimed at sensor semantic interoperability in Environmental/Cities/Water domains (more relevant ones). [Information harmonization at semantic level in form of OGC standards]
* **Linked Building Data (European):** Focused on treating the semantics since the building life cycle perspective. Focusing on IoT on buildings (operational stage) they are immerse on the elaboration of a "ontology recommendation tool" based on the experience of latest H2020 projects.
* In terms of standardization, OGC is the "more formal" association in this sense (as far as I know). ETSI has published some documents regarding the landscape of data models for diverse domains. In Europe, AIOTI could be the organization of publishing and promoting "IoT semantic interoperability" in a formal way too.

**Answer to Question 1 (on Open Mobile Alliance (OMA)) provided by Hannes Tschofenig Hannes.Tschofenig@ARM.COM**

The Open Mobile Alliance (OMA) has developed a protocol, called LwM2M, for managing Internet of Things (IoT) devices to address a number of challenges, including

* letting customers control their devices in a (near) real-time fashion over the internet.
* collecting sensor data from these devices securely so that value-added services, such as analytics, can be provided.
* updating the software of these devices once they are deployed.
* obtaining statistics and trouble-shooting information to determine failure causes and to offer customer support when devices malfunction.
* managing these devices over their lifetime, including the provisioning of security credentials and distribution of access control lists, to ensure that only entitled parties can access sensitive data.

OMA is currently finalizing version 1.0 of the LwM2M specification based on the input from various interoperability events. The specification can be downloaded from the [OMA webpage](http://technical.openmobilealliance.org/Technical/technical-information/release-program/current-releases/oma-lightweightm2m-v1-0). Work on version 1.1 has been started and aims to provide features like

* + Support for [CoAP over TCP/TLS](https://tools.ietf.org/html/draft-ietf-core-coap-tcp-tls-04)
  + Protocol gateway support
  + Support for additional transports, such as HTTP/2.
  + Additional security features, such as [DTLS IoT profile compliance,](https://tools.ietf.org/html/rfc7925) [TLS 1.3 support](https://tools.ietf.org/html/draft-ietf-tls-tls13), application layer security, and new bootstrapping modes.
  + Support for low power WANs, such as the 3GPP NB-IoT.

Contributing to the work on LWM2M is easy.

To contribute to the technical specification

* + Submit new objects to the [repository](http://technical.openmobilealliance.org/Technical/technical-information/omna/lightweight-m2m-lwm2m-object-registry).
  + File issues with the [public OMA LWM2M Github issue tracker](https://github.com/OpenMobileAlliance/OMA_LwM2M_for_Developers/issues).
  + Become [OMA member](http://openmobilealliance.org/membership/) and participate in the standardization process.
  + Participate in the IETF for foundational standards (such as CoAP, DTLS/TLS, HTTP, etc.)

To contribute code

* + Several open source projects are happy to receive your contributions.
  + Examples: [ARM mbed client](https://github.com/ARMmbed/mbed-client), [Leshan](https://github.com/eclipse/leshan) and [Wakaama](https://github.com/eclipse/wakaama)

To test your implementation:

* Join an interoperability test event (PlugFest, TestFest). Info about upcoming events can be found at the [OMA testfest website](http://technical.openmobilealliance.org/Technical/testfest-overview).
* Use one of the available open source implementations to test against.

**Question 2: Where do we want to go?**

**Individual answers from AIOTI WG03 members (not necessarily representing opinion(s) of the company/organisation that the AIOTI WG03 member is working for):**

**Question 2.a: What kinds of next-generation platforms are needed (if any)?**

**Individual answers from AIOTI WG03 members (not necessarily representing opinion(s) of the company/organisation that the AIOTI WG03 member is working for)**

**Answer to Question 2.a provided by Juergen Heiles (**[**juergen.heiles@siemens.com**](mailto:juergen.heiles@siemens.com)**)**

<JH>: The first issue is what kind of platforms are considered? The UNIFY document provides an overview of existing IoT platforms which provide different levels of functionality (e.g. device centric, communication centric, data centric, ...). In addition you can think of operating systems as platforms for  application development, of market platforms for offering of services, goods, even data. An example for the later is the Industrial Data Space activity (<http://www.industrialdataspace.org/en/>) in Germany. Industrial Data Space is a vir­tual data space which supports the secure exchange and simple lin­king of data in business eco­systems on the basis of standards and by using collaborative governance models.

The question itself is a market and business issue. Standardization bodies define standards based on market needs.  So I am not sure what to answer from a WG03 perspective. STF505 has identified gaps for specific technology and other topics, but none that talks about specific needs for platforms. I would expect to get answers from the AIOTI vertical WGs as they should look on the needs of their application areas.

**Answer to Question 2.a provided by Omar Elloumi (omar.elloumi@nokia.com)**

OE> Instead of thinking about the next generation platforms, the main focus should be about consolidation around EU championed platforms from R&I and standards. As we move from single domain IoT to cross domain IoT, the focus should shift to a system of system (or system to system) approach where pivotal points of interoperability (cf. NIST CPS) can be used to interoperate at large scale. There are two important enablers for this shift in focus: semantic interoperability (which is not yet understood nor widely adopted) and data sciences to extract value out of big data generated by IoT.

**Answer to Question 2.a  provided by Emmanuel Darmois (for STF 505)**

Recently, oneM2M has emerged as a global platform for the IoT/M2M Service Layer with a very large support of various actors in the IoT value chain. IoT applications providers are more and more providing solutions to interwork with oneM2M platform. A very large number of developers of solutions at the IoT Service Layer are offering or plan to offer plugins for oneM2M platform, thus expending the reach of the Service Layer platform itself. In addition, several Open Source communities have developed various implementations - or parts - of oneM2M, thus providing additional support for a new range of services using Open Source. Altogether, it is now clear that oneM2M is a winner at the Service Layer, with a breadth of services that few – if no – competitors can offer. The investment done by the oneM2M members and the IoT community at-large around the oneM2M platform is really beginning to pay off. In this sense, chances are that the next-generation platforms will rely on – and expand – the oneM2M platform rather than compete with it.

**Answer to Question 2.a provided by Davide Brandano (davide.brandano@APPLUS.COM)**

DB: we need secure and interoperable platforms, across different technologies and domains. I aware I am saying something obvious, but maybe not so obvious considering that, especially regarding security, the most is currently missing. Off course there are a lot of efforts to be done, lot of bodies are afraid in putting the first brick (that is, the first €) in order to overcome this lack of security in IoT communications, since they do not want take the risk of supporting all the required efforts. The question is: who has more to lose in “non-secure” IoT communication? Which actors of the chain? That one should put the most of the effort, and it is not the final user. I guess we are now in the moment to priories the security in IoT, because while the benefits of the objects are clear, what is true is that security has not, currently, the same rhythm of related IoT innovation.

**Answer to Question 2.a provided by Georgios Karagiannis (**[**georgios.karagiannis@huawei.com**](mailto:georgios.karagiannis@huawei.com)**) – AIOTI WG03 vice-chair**

Georgios: The Unify IoT project report that is focusing on IoT platforms provides recommendations on the types of the next generation platforms that are needed. AIOTI WG03 will use this report and will elaborate on the derived conclusions from this report. In particular, regarding the next generation IoT platforms, currently, the providers of IoT platforms are fragmented. In the near future, there is a need to design overarching, integrated IoT platforms that bring the devices, networks and endpoints together in the companies' and IoT ecosystems that develop various IoT applications. This means that in this context, the IoT platforms need to be and act as a complete IoT/IT/OT ecosystem converging the consumer/business/industrial applications by collecting and sharing data broadly within an organization, sectors, and IoT applications. This need to be converted into an IoT platform strategy, based on open specifications, strong interoperability principle, security and standardization. The strong interoperability principle should be applied not only within one IoT platform, but also between different IoT platforms, assuming that more than one IoT platforms will need to cooperate with each other in order to support innovative services and applications.

**Answer to Question 2.a (on where we want to go?) provided by Harris Moysiadis [mailto:tmoysiadis@f-in.gr]**

HM: I guess to rapid, decentralised but coordinated IoT paradigms that could drive technological and social innovation further. And also with an assessment list of what could have been done in another way and why (an impact approach). 

**Answer to Question 2.a (IoT Semantic Interoperability) provided by Aitor Corchero Rodriguez (**[**aitor.corchero@EURECAT.ORG**](mailto:aitor.corchero@EURECAT.ORG)**)**

In terms of next generation platforms, scientific and industrial movements are focusing on elaborating common architectures to integrate and fuse information under a common visualization. Specifically some of the trends are focused on (i) Linked Data platforms for Sensors; (ii) Spatial-temporal reasoning architectures.

**Question 2.b: What kinds of large-scale federating initiatives are needed (if any)?**

**Individual answers from AIOTI WG03 members (not necessarily representing opinion(s) of the company/organisation that the AIOTI WG03 member is working for):**

**Answer to Question 2.b provided by Juergen Heiles (**[**juergen.heiles@siemens.com**](mailto:juergen.heiles@siemens.com)**)**

<JH> Not sure, do we have something in the gaps that requires federating initiatives. Identity federation is an issue an activities are ongoing. Should we thing of semantics federation?

**Answer to Question 2.b provided by Omar Elloumi (omar.elloumi@nokia.com)**

OE> Semantic interoperability for cross domain IoT could be a good example of a federating initiatives (and there are certainly others). It should not aim at creating new ontologies (there are way too many out there), it should focus on creating industry-wide consensus on fewer sets of ontologies and related tools that could be applied consistently. Policy actions related to market/engineering education and possibly interop event or certification programs can greatly support this vision.

**Answer to Question 2.b provided by Davide Brandano (davide.brandano@APPLUS.COM)**

DB: I need more time for thinking about which federating initiatives should be needed. I agree with Jurgen that it is an on-progress issues, but not clear regarding the timing needed.

**Answer to Question 2.b provided by Georgios Karagiannis (**[**georgios.karagiannis@huawei.com**](mailto:georgios.karagiannis@huawei.com)**) – AIOTI WG03 vice-chair**

Georgios: According to the Unify IoT report on IoT platforms, the creation of a single digital market for IoT requires federated market places across currently emerging IoT platform silos. By enabling re-use of assets across different IoT ecosystem boundaries, secondary revenue streams can be generated for IoT infrastructure investments, which will boost the overall IoT market. The large-scale federating initiatives should have as goal the support of cross-domain IoT solutions.

**Answer to Question 2.b provided by Valentijn de Leeuw (Gérant) [mailto:Valentijn@kyoyu-sha.eu]**

<VVdL> we should have an overarching activity that keeps checking if individual LSP’s remain compatible and interoperable

**Answer to Question 2.b (IoT Semantic Interoperability) provided by Aitor Corchero Rodriguez (**[**aitor.corchero@EURECAT.ORG**](mailto:aitor.corchero@EURECAT.ORG)**)**

In terms of federative semantic architectures for IoT (if this question refer to that, I am not sure), there are one initiative named as Fiesta-IoT project (<http://fiesta-iot.eu>).

**Question 2.c: What concrete gaps/problems could be addressed through platform development and large-scale initiatives at EU level?**

**Individual answers from AIOTI WG03 members (not necessarily representing opinion(s) of the company/organisation that the AIOTI WG03 member is working for):**

**Answer to Question 2.c provided by Juergen Heiles (**[**juergen.heiles@siemens.com**](mailto:juergen.heiles@siemens.com)**)**

<JH>: STF505 has identified gaps, but can they be addressed through platform development? Large-scale initiatives at EU level like LSPs and other research activities for sure can consider the gaps and may provide solutions that fill the gap and could contribute to standardization. However such work will not be driven just by standardization gaps.

**Answer to Question 2.c provided by Omar Elloumi (omar.elloumi@nokia.com)**

OE>

* Cloud hosting and network related SLA (service level agreement)
* Platform independent SDKs
* Barriers (including funding) to commercial deployments in particular for smart cities (which remain largely policy funded)
* Evolution of device management platforms (including related security)

**Answer to Question 2.c provided by Emmanuel Darmois (for STF 505)**

The gaps of IoT as they are detailed in the STF 505 report (ETSI Technical Report TR 103 376) are not just technical, which means that they do not only concern standardization gaps. Other important gaps can refer to business and societal concerns, the latter including very important issues such as security or privacy.

The major areas for gaps are:

* + Data Interoperability. A first example related to the lack of easy translation mechanisms between different specific models, not to mention the need for global data model. Another example is related to the harmonization (standardization?) of high-level behavioral messages (e.g., alerts, alarms) that would enable a better understanding by those who receive them.
  + Service Platform. No obvious winner can be seen amongst all IoT HLAs. However, the recent IoT/M2M workshop held in ETSI (in November 2016) has shown that oneM2M is emerging as a global platform that has gained a very large support of various actors, such as IoT applications providers (that want to interwork with oneM2M platform), developers of specific solutions at the Service Layer (that will offer plugins for oneM2M) or Open Source communities (that have developed various implementations - or parts - of oneM2M).
  + Security and Privacy. In order to make sure that the full business potential of IoT can be reached, IoT platforms have to ensure data privacy, integrity and transmission in accordance with the information sensitivity. Many vertical domains require solutions for this, in particular from standards. As an example, Smart Environment actors (e.g., utilities such as energy or water) can delay large-scale deployments as long as such standards and solutions are lacking. Similarly, privacy and security issues can be a blocking factor for use acceptance in Wearables.
  + Usability. Users often find that IoT systems are not enough simple to set-up and use (especially compared to other systems specifically designed for them). This is a problem for most of the vertical domains, e.g., Smart Home or Wearables. Some support from Standards may help improve user acceptance.
  + Sensor Quality and Reliability. A variety of sensors are developed without proper guidelines regarding Quality and Reliability and may not have final characteristics that correspond to the expectations. A pressing need for standards to define criteria to assess those aspects is emerging. Such standards may come in support of IoT devices conformance assessment.

When it comes to the development of systems or applications, security and privacy are addressed on a very specific basis, often without a close involvement of security experts: security by design – which is expected to overcome this – is still at early stages: standards and, more importantly, education are needed to improve the global expertise of system and applications developers.

The business and societal gaps – though not the subject of standardization activities – are important issues for the IoT industry as well as for the identification of potential improvements regarding regulatory of legal frameworks. This is clearly the case for privacy issues: it is now generally considered that these issues will be dealt with primarily at the regulatory level, more than at the technical one.

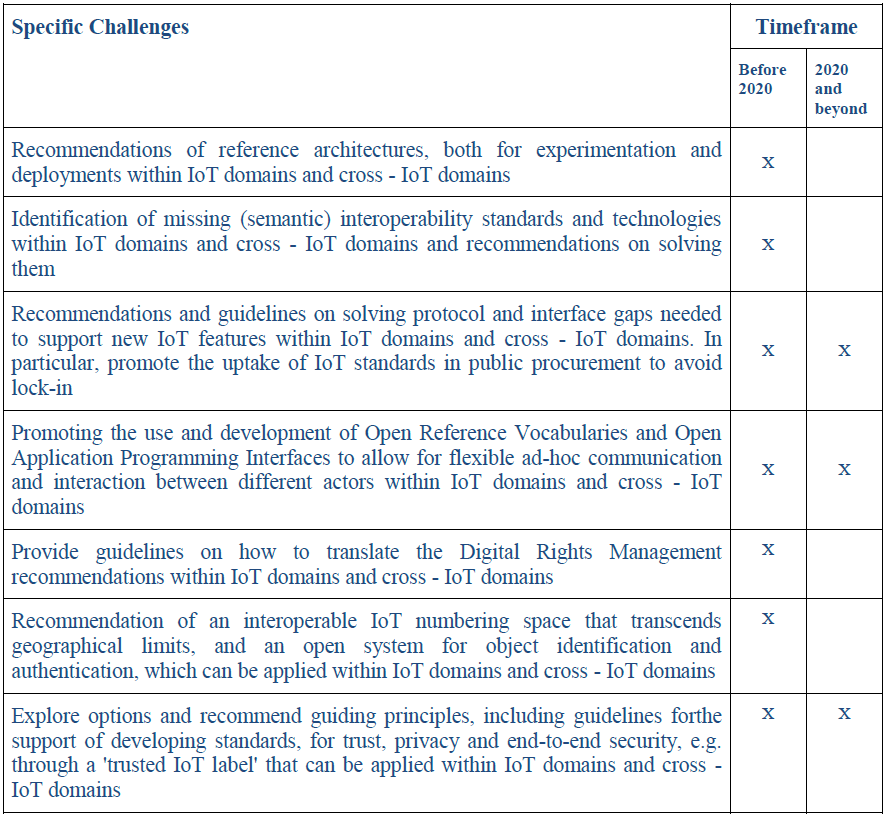
**Answer to Question 2.c provided by Davide Brandano (davide.brandano@APPLUS.COM)**

DB: The best should be  to address all theses issues from LSPs, with huge impact in the society: I think that finding LSP with big impact in the society is a very important topic: the output of LSP should not only have an impact on the involved insiders… As a consequent step,  the standardization bodies can act using the output of the LSP. Gaps/problems to be addressed, in my opinion, are related to interoperability and security across different technologies and domains.

**Answer to Question 2.c provided by Georgios Karagiannis (**[**georgios.karagiannis@huawei.com**](mailto:georgios.karagiannis@huawei.com)**) – AIOTI WG03 vice-chair**

Georgios: According to the UNIFY-IoT IoT platform report there are several gaps still existing both on technology and business models. One of these gaps is the support for integrated cloud, mobile edge computing and edge analytics solutions in current IoT platforms. Another one is the lack of 3rd party market places inside of the current IoT platforms and in particular the lack of component developers, since this can be considered as a crucial element to stimulate the success that we know of the app economy in the mobile world. The third gap mentioned by the same report is related to the requirements that are imposed by emerging industrial IoT applications, Tactile Internet and autonomous/robotic systems solutions that require much faster reactivity at the edges of the networks. In order to support these requirements, analytics algorithms will have to operate in a distributed context between edges and cloud with heterogeneous capabilities. Moreover, much more sophisticated frameworks in place are required to enable effective synchronisation and adaptability.

Furthermore, AIOTI WG03 focuses on gaps in IoT standardization derived from IoT landscape analysis by exploiting as much as possible the results of recent projects, including Large Scale Pilots. In particular, AIOTI WG03 is aiming for (1) consolidation of architectural frameworks, reference architectures, and architectural styles in the IoT space, (2) (semantic) interoperability, (3) security and (4) personal data & personal data protection to the various categories of stakeholders in the IoT space. In addition, AIOTI WG03 focuses on the specific challenges mentioned in the below table.



**Answer to Question 2.c provided by Valentijn de Leeuw (Gérant) [mailto:Valentijn@kyoyu-sha.eu]**

<VVdL> Industry is developing IoT based eco-system collaboration between operators-owners, service providers and vendors for equipment and process monitoring, support and predictive analytics.  Another area of collaboration is IoT based supply chain collaboration.  Solutions tend to be developed on top of vendor platforms for IoT.  Once the first wave of applications become available, the next wave will be the integration of those, among each other and with applications for traffic, cities, energy supply and others. This is a critical phase for interoperability.  The integration nightmare of production systems in industry over the past 20 years (ISA-95) needs to be avoided, and instead plug an play operability is highly desirable.  Again standards-based platforms could avoid these challenges. See also the report referenced below: "Unify IoT project” ICT-30-2015: Internet of Things and Platforms for Connected Smart Objects”

**Answer to Question 2.c (IoT Semantic Interoperability) provided by Aitor Corchero Rodriguez (**[**aitor.corchero@EURECAT.ORG**](mailto:aitor.corchero@EURECAT.ORG)**)**

Main gap/problems to be tacked under the development of this kind of architectures could be:

* **Each architecture have their own APIs to integrate information and abstract the information**. Regarding with this problem, the challenge is to develop common and harmonize APIs to integrate the information.
* **Multiple domain specific semantic models**. There exist numerous ontologies for diverse domains regarding IoT representation. Then, the challenge could be to unify these models or promoting/proposing models from the Linked Open Vocabularies.
* **There is no effective mechanism to perform semantically temporal and spatial querying and knowledge generation (reasoning)**. Enabling temporal and spatial reasoning over the information in terms of RSPs (RDF Stream Processing) could permit to derive relevant information at same time as continuously integrating the generated data/information (continuous flows of information).
* **Semantic storage querying performance decay at large scale (high quantity of axioms)**. The challenge could be to limit the information to be stored in the semantic data storage depending the interest or even limit the reasoning capabilities.

**Question 3: How do we bridge the gap between what we have and what we want to achieve? Where to focus?**

**Individual answers from AIOTI WG03 members (not necessarily representing opinion(s) of the company/organisation that the AIOTI WG03 member is working for):**

**Answer to Question 3 provided by Juergen Heiles (**[**juergen.heiles@siemens.com**](mailto:juergen.heiles@siemens.com)**)**

<JH>: That needs further elaboration when we have an answer on what we want to achieve concerning platforms and other topics

**Answer to Question 3 provided by Omar Elloumi (omar.elloumi@nokia.com)**

**OE>**

* Platform winners and losers is a largely not needed debate, the focus should be about system of system (or system to system) approach and getting semantics and big data to work to the advantage of EU industries.

**OE> Regarding High Level Architecture (HLA) :**

* The main advantage of HLA is to have a common understanding of the concepts among the large set of players which come from different background (universities, industries, policy, etc.). If we evolve the HLA in the right manner we will ensure that all the stakeholders speak a common language making it easier to reach common understanding and consensus about:
  + Gaps
  + Comparing platform features
  + Identifying interoperability points
  + Discussing and influencing SDOs and possibly open source initiatives (in a favorable direction)
  + Building consolidated/coordinated roadmaps

**OE> > Regarding IoT Semantic Interoperability**

* There is a great danger for semantic interoperability (ontologies and reasoning) to remain at research labs. As we recommended during the first version of the AIOTI semantic interop delibrable, we should be exploring ways to educate the market and the engineers about the benefits and their use in operational deployments. Additionally we should create the conditions for achieving consensus/consolidation around a ontologies and related tools in direct relation to LSPs and or projects.
* The link between semantic and big data may need further exploration.

**Answer to Question 3 (Regarding High Level Architecture (HLA)): provided by Emmanuel Darmois (for STF 505)**

A number of the generic standards that have been identified in the STF 505 report on IoT Standards Landscaping are related to IoT High Level Architecture models. All these standards exist for various reasons, amongst which a concurrent development in various SDOs or a different origin (e.g., a specific vertical domain). To a large extent, these standards bear strong resemblance and significant differences. For the sake of interoperability between systems based on different architectures, it is important that any of these HLA standards can be mapped onto any other. These mappings should be supported by the "platforms" that are adhering to one of these HLAs.

**Answer to Question 3 provided by by Davide Brandano (davide.brandano@APPLUS.COM)**

DB: First of all we should agree and converge onto what really we need, more or less it is what Jurgen has already  addressed: according my point of view previously mentioned, we need to focus onto security layers ensuring interoperability. It supposes a big level of dedications and efforts, but the key issue is: who has to leader it?

**Answer to Question 3 provided by Francois Ennesser (Francois.Ennesser@gemalto.com)**

**“IoT Security & Privacy recommendations”:**

* The basis to secure IoT systems is to perform an exhaustive **Risk Assessment** for each deployment.
* This should involve all relevant stakeholders. There are already regulatory guidelines and established processes to support this.
* But in IoT, more than in traditional ICT systems, special attention should be paid to the following two **risk domains**:
  1. **Privacy:** This is especially a concern for Consumer oriented IoT applications and can be mitigated mainly by securing the INPUTS of the IoT information processing system, which typically contain information about our own individual behavior. Extending Risk Assessment to privacy is already supported by Privacy/Data Protection Impact Assessment templates made available by regulators for typical use cases (RFID, Smartgrid…).
  2. An at least as important area that should not be bypassed in risk assessments, and does not appear much in our current work, is **safety, i.e. the adverse effect that the IoT system may have on its environment.** *While this is not a concern in traditional ICT systems, controlling actuators that physically impact the system environment (e.g. heaters or power transformers) is the primary purpose of IoT systems*, and is a main concern for Industrial IoT applications. Sending wrong outputs to actuators can result in physical damages to the environment (e.g. explosion of a transformer whose input and output powers become unbalanced), potentially resulting in human casualties. This makes such systems an attractive target for hostile organizations such as foreign powers able to invest important means to perform an attack. And mitigating such threats imply securing the entire IoT information processing chain, from inputs to outputs (security is a chain that is only as strong as its weakest link). Perhaps some kind of “Safety Impact Assessment” template should be considered by regulators to address this area? Existing EU work on Critical Infrastructures Protection such as ERNCIP (under DG Home) could be relevant here.

Furthermore, we have already seen how unsecure IoT devices can be exploited to disrupt traditional internet services. The consequences of such attacks will be more dreadful when they will be misused to disrupt IoT systems such as smartgrids. This is why the proposed notion of an “IoT Trust Label” setting minimal requirements to ensure good “social cohabitation” of connected ICT systems should not be discarded.

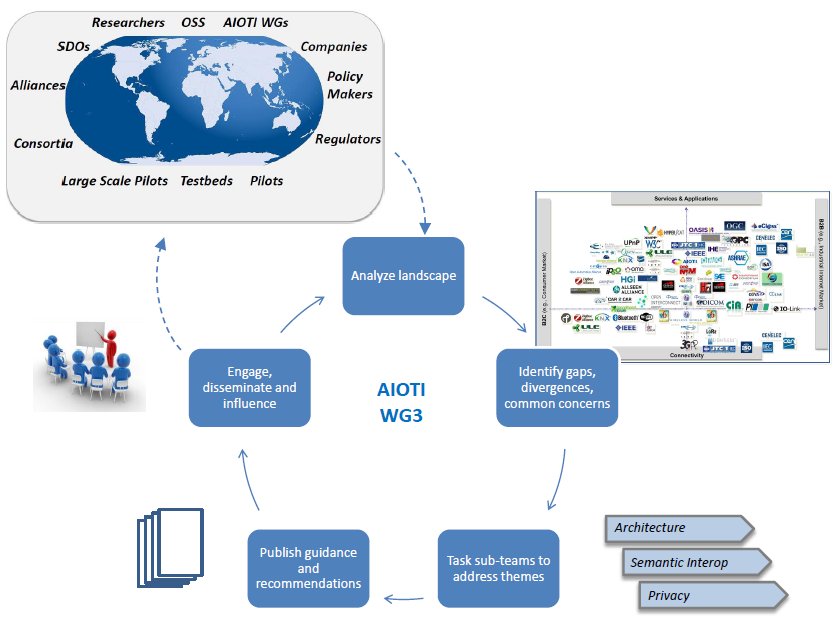
**Answer to Question 3 provided by Georgios Karagiannis (**[**georgios.karagiannis@huawei.com**](mailto:georgios.karagiannis@huawei.com)**) – AIOTI WG03 vice-chair**

Georgios: This depends on the type of the gaps. Some gaps can be solved by involving regulation and policy makers. Other gaps have a technical nature and can be solved by standardisation and Go To Market activities.

Important to emphasize that AIOTI WG03 will not develop any standards nor open source implementation. Therefore, it is important to engage, cooperate and influence other SDO, Alliance and Open Source initiatives to work on the gaps identified by AIOTI and promote standardization solutions for these gaps.

This figure shows the engagement model that the AIOTI WG03 is planned to follow for the future, which:

* Maintains a view on the landscape of IoT standards-relevant activities being driven by SDOs, Consortia, Alliances and OSS projects, Researchers, Companies, Policy Makers, Regulation, Testbeds and Pilots.
* Provides a forum for analysis, discussion and alignment of strategic, cross-domain, technical themes and shared concerns across landscape activities
* Develops recommendations and guidelines addressing those concerns and engages the broader IoT community in disseminating and promoting the results
* Evolves the AIOTI High Level Architecture in collaboration with other AIOTI WGs



**Answer to Question 3 provided by Valentijn de Leeuw (Gérant) [mailto:Valentijn@kyoyu-sha.eu]**

<VVdL> agreed with answer provided by Juergen Heiles: That needs further elaboration when we have an answer on what we want to achieve concerning platforms and other topics

**Answer to Question 3 (IoT Semantic Interoperability) provided by Aitor Corchero Rodriguez (**[**aitor.corchero@EURECAT.ORG**](mailto:aitor.corchero@EURECAT.ORG)**)**

Regarding this question and as a personal opinion (to be discussed of course) maybe a unified and cross-domain architecture combining semantics and IoT could be promoted (initial thoughts were done under HLA group, I think).

**Question 4: Who are the main stakeholders to be involved?**

**Question 4.a: How can industrial partnerships (such as PPPs or AIOTI) contribute to building platforms?**

* **Individual answers from AIOTI WG03 members (not necessarily representing opinion(s) of the company/organisation that the AIOTI WG03 member is working for):**

**Answer to Question 4.a provided by Juergen Heiles (**[**juergen.heiles@siemens.com**](mailto:juergen.heiles@siemens.com)**)**

<JH>: Standardization will not define the platforms, but it can support them by providing standards for specific technologies, protocols, especially the underlying infrastructure (e.g. communication

**Answer to Question 4.a provided by by Davide Brandano (davide.brandano@APPLUS.COM)**

DB: Pushing on LSP definition and realization, always considering the huge impact on the society as a must. Then, SDOs can support on these activities, but basing on LSPs outputs (also partial outputs, during LSP execution).

**Answer to Question 4.a provided by Georgios Karagiannis (**[**georgios.karagiannis@huawei.com**](mailto:georgios.karagiannis@huawei.com)**) – AIOTI WG03 vice-chair**

Georgios: This can be done by helping to solve the identified gaps using an engagement model as the one explained in the answer above.

In principle all the stakeholders that are needed in the IoT value chain, which are various types of stakeholders, i.e., industries that focus on vertical domains, horizontal industries, such as telecom operators and telecom vendors, large companies, Industrial IoT, Consumer IoT, Enterprise IoT, Startups, SMEs and Academia, regulation, policy makers, SDOs, Alliances, OSSs, LSPs, Testbeds, Pilots.

**Answer to Question 4.a (on where we want to go?) provided by Harris Moysiadis [mailto:tmoysiadis@f-in.gr]**

HM: Public organisations (regulatory bodies, operators/ distributors where applicable for final business requirements), Private (industry to co-invest and strategy, SMEs for hands on), Research Organisations to close the learning loop of the initiative.

**Answer to Question 4.a provided by Valentijn de Leeuw (Gérant) [mailto:Valentijn@kyoyu-sha.eu]**

<vvdL> we need to reach out to defect open-source standards and collaborate in my view.

**Answer to Question 4.a (IoT Semantic Interoperability) provided by Aitor Corchero Rodriguez (**[**aitor.corchero@EURECAT.ORG**](mailto:aitor.corchero@EURECAT.ORG)**)**

The PPPs or AIOTI could provide the following:

* Standards/Guidelines/Best practices.
* Specific technology.
* Test-beds or Evaluations (of technology for example).

**Question 4.b Why Countries need National IOT strategies? What governments must do for building platforms?**

**Individual answers from AIOTI WG03 members (not necessarily representing opinion(s) of the company/organisation that the AIOTI WG03 member is working for)**

**Answer to Question 4.b provided by Juergen Heiles (**[**juergen.heiles@siemens.com**](mailto:juergen.heiles@siemens.com)**)**

<JH>: That is a policy and not a standardization question. Do we expect that governments shall drive standardization? So far standardization is a public issue with government involvement mainly for regulatory topics.

**Answer to Question 4.b provided by Omar Elloumi (omar.elloumi@nokia.com)**

OE>

* This could be a good subject for exploration, we see great potential pertaining to e.g. India 100 smart cities project initiatives. This is recognizing two roadblocks: funding and lack of resources and expertise to source new platform based solutions. Platform enabled smart cities remains a big challenge for different reasons, without solving this challenge (not only technical), the vision of smart cities may never be reached.

**Answer to Question 4.b provided by Arthur van der Wees [mailto:vanderwees@arthurslegal.com]**

[\*Arthurslegal: any member state should have a – detailed and fine-grained – digital agenda and strategy, which include IoT, cloud computing, data analytics, and the like, both on horizontal levels as well as vertical markets, both existing and new. This, simply in order to boost and foster productity, employability, social inclusion, and many other national topics in society and economy. Too generic may work on EU level to a certain extent, but not on a national, practical level. It would be excellent if they should not be required to invent the wheel, make painful mistakes that others also have made, and would be great if they can leverage on best practices, guidelines, self-regulatory initiatives, regulations and other legal framework instruments and baselines. The EU broad approach, and preferably even a global approach – as technology is global and ignores borders – (without waiting for global consensus, as technology and innovation is at supersonic speed already). National strategies help for instance with getting technology, platforms and other ecosystems to its part of the market and 520 million EU citizens. Silo-ed and non-transparant strategies will not help, is too slow to get to market, and costs to much resources without giving it a chance to market and societal adoption and success. Converging the combined knowledge, capabilities and ability to execute on EU level will help establish future-proof standards & legal framework, understandable and easy to understand Rule of Law, for purposes to expedite such adoption and success. AIOTI supports exactly with that, on an all-partisan level.]

**Answer to Question 4.b provided by by Davide Brandano (davide.brandano@APPLUS.COM)**

DB: Policy (locally but driven and according EU macro-initiatives) must support and foment initiatives, pilots, etc. But standardization issues should be complementary to those polices. Policy must push on and support in creating the case studies, in order that standardization can act onto.

**Answer to Question 4.b provided by Georgios Karagiannis (**[**georgios.karagiannis@huawei.com**](mailto:georgios.karagiannis@huawei.com)**) – AIOTI WG03 vice-chair**

Georgios: This is more a policy related question. In particular, is important that national and international regulation should not block innovation. Governments should help to alleviate the barriers for the large scale deployment of IoT, such as alleviating the obstacles that enable the Free Flow of IoT data across national borders, see AIOTI WG04 policy paper.

**Answer to Question 4.b provided by Valentijn de Leeuw (Gérant) [mailto:Valentijn@kyoyu-sha.eu]**

VVdL> governments should promote standardization, for the same reason as they should promote international trade: increased economic growth

**Answer to Question 4.b (IoT Semantic Interoperability) provided by Aitor Corchero Rodriguez (**[**aitor.corchero@EURECAT.ORG**](mailto:aitor.corchero@EURECAT.ORG)**)**

I think this question is more regarding policy. Even though, the elaboration of an IoT strategy could be beneficial to the governments to promote and serve to the citizens services and information at same time as inter-connecting domains between them.

**Question 4.c How to maximise benefits through coordination at European level?**

**Individual answers from AIOTI WG03 members (not necessarily representing opinion(s) of the company/organisation that the AIOTI WG03 member is working for):**

**Answer to Question 4.c provided by Juergen Heiles (**[**juergen.heiles@siemens.com**](mailto:juergen.heiles@siemens.com)**)**

<JH>: For us standards should be international and not regional. Still a common European voice in international standardization will be useful.

**Answer to Question 4.c provided by Omar Elloumi (omar.elloumi@nokia.com)**

OE>

* There’s a lack of transfer of research results into standards, often research projects attend a standards meeting, make a presentation then go home… there a need to enhance the transfer process from research to standards.

**Answer to Question 4.c provided by Arthur van der Wees [mailto:vanderwees@arthurslegal.com]**

[\*Arthurslegal: Reference is made to my comments above. The fine-graining of higher level standards is important, and any EU or other international coordination should take that into account: the output of the efforts must be easy to understand, implement and give room for fine-graining and innovation. Basically, EU coordination should preferably be designed to be interoperable, lean and agile.]

**Answer to Question 4.c provided by by Davide Brandano (davide.brandano@APPLUS.COM)**

DB: Common and shared guidelines from EU are needed. Standardization must act as upper level, in harmonized and shared way for all EU.

**Answer to Question 4.c provided by Georgios Karagiannis (**[**georgios.karagiannis@huawei.com**](mailto:georgios.karagiannis@huawei.com)**) – AIOTI WG03 vice-chair**

Georgios: Several areas can benefit through coordination at European level.

* An important area is standardisation. The support of SDOs at European level gives the possibility to develop IoT standards that have a significant impact on the European and as well as on the global IoT ecosystem.
* Another area is regulation, where the Member States can be consulted in an effort to prevent the creation of barriers that will harm the IoT deployment in Europe and globally.
* Another area is the coordination of the research and innovation in Europe, where cooperation between Member States and international actors can be considered as an integral part.

**Answer to Question 4.c provided by Valentijn de Leeuw (Gérant) [mailto:Valentijn@kyoyu-sha.eu]**

<VVdL> agreed on the importance of international, however the more united and consistent we are, the more weight will our voice have.

**Answer to Question 4.c (IoT Semantic Interoperability) provided by Aitor Corchero Rodriguez (**[**aitor.corchero@EURECAT.ORG**](mailto:aitor.corchero@EURECAT.ORG)**)**

At European level, the benefits could be maximized through promoting standards, best practices, technology aligned to the semantic interoperability in IoT domains.