AIOTI

ALLIANCE FOR INTERNET OF THINGS INNOVATION

IoT LSP Standard Framework Concepts

Release 2.0

AIOTI WG03 – IoT Standardisation

2015

Executive Summary

This deliverable introduces IoT Standards Developing Organisation (SDO), Alliance and Open Source Software (OSS) landscapes to be used as input for the recommendations for Large Scale Pilots (LSPs) standard framework and gap analysis. The LSPs can play an important role in investigating and solving specific challenges for the IoT industry and promoting innovation that is related to specific activities such as 1) the applied standards framework, 2) deployments, 3) technological and business model validation and 4) acceptability.
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: 1) to leverage on existing IoT standardization, industry promotion and implementation of standards and protocols, 2) as input for LSP 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.

Table of Contents

1. GOAL AND MOTIVATION 4

2. IOT SDO AND ALLIANCE INITIATIVES LANDSCAPE 5

3. IOT OPEN SOURCE SOFTWARE INITIATIVES LANDSCAPE 7

4. MAPPING SDO/ALLIANCE/OSS/ INITIATIVES INTO KNOWLEDGE AREAS 8

5. APPENDIX 1: IOT SDOS, ALLIANCES AND OSSS 10

5.1 SDO, ALLIANCE, AND OSS INITIATIVES TEMPLATE FOR INFORMATION COLLECTION 10
5.2 IOT SDO/ALLIANCE INITIATIVES 12
5.2.1 3GPP (3rd Generation Partnership Project) 15
5.2.2 AVNU Alliance 17
5.2.3 BBF (Broadband Forum): Broadband User Services (BUS) Work Area 19
5.2.4 ETSI (European Telecommunications Standards Institute) 21
5.2.5 GSMA (GSM Association) 47
5.2.6 HyperCat 49
5.2.7 IEC (International Electrotechnical Commission) 50
5.2.8 IEEE P2413: Standard for an Architectural Framework for the Internet of Things 55
5.2.9 IETF (Internet Engineering Task Force) 56
5.2.10 IRTF (Internet Research Task Force): T2T RG (Thing to Thing) proposed RG 74
5.2.11 International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) 76
5.2.12 (ISO/IEC) JTC1/WG10 Internet of Things 79
5.2.13 OIC (Open Interconnect Consortium) 81
5.2.14 OneM2M 83
5.2.15 OSGi Alliance 86
5.2.16 Weightless 90
5.2.17 WWRF (Wireless World Research Forum) 90
5.3 IOT OSS INITIATIVES 92
5.3.1 IoTivity 93
5.3.2 OM2M (Open platform for M2M) 95
5.3.3 sensiNact (aka BUTLER platform) 96

6. APPENDIX 2: TECHNOLOGY TRENDS FOR THE SUPPORT OF IOT 100

6.1 WIRELESS CONNECTIVITY TRENDS FOR THE SUPPORT OF IOT 100

7. REFERENCES 100

1. Goal and motivation

The IoT is becoming a market reality. However, in order to meet the IoT expectations such as a) leveraging on hyper-connectivity, b) enabling interoperability of solutions and semantically enriched information distributions and c) facilitating object and data reuse across application domains, several challenges need to be addressed. In particular, three of the challenges that are associated to LSPs (Large Scale Pilots) are: 1) large number of competing technology standards, which are projected in both horizontal and vertical directions, 2) lack of understanding of new business models and 3) social questions. The vertical direction implies that the standards and protocols are developed for the support of applications/services that are belonging to a particular application domain, i.e., a single vertical industry, such as home automation, smart mobility and wearable medical devices, etc. The horizontal direction implies that the standards and protocols are not targeting a specific vertical industry, but aim at providing general standard, protocols and solutions for as many vertical industry types as possible with the implication of developing limited adaptations to the applications that they need to support.

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, which can be used: 1) to leverage on existing IoT standardization, industry promotion and implementation of standards and protocols, 2) as input for LSP 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.

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).

2. IoT SDO and Alliance Initiatives Landscape

This section briefly introduces main IoT SDO and Alliance initiatives that have a worldwide visibility and applicability and provides the global landscapes associated with these SDO and Alliance initiatives.

Figure 1 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.

The projection of these initiatives on these two dimensions has been accomplished based on discussions among experts participating in both AIOTI WG03 and relevant initiatives as well as on the collected information presented in Appendix 1 (Section 5).

Figure 1: IoT SDO and Alliances Landscape

In addition to the SDO and Alliance landscape shown in Figure 1, a projection of these initiatives into vertical industry domains is shown in Figure 2. The "IoT SDOs and Alliances Landscape (Vertical and Horizontal Domains)" is a graphical representation aiming to highlight the main activity (up to the day of generating this representation) of SDOs and Alliances with respect to the IoT application domains represented as "verticals" and the IoT Telecommunication Infrastructure domain represented as "Horizontal/Telecommunication".

Figure 2: IoT SDO and Alliance Initiatives Projection on Vertical and Horizontal Domains

The landscapes described in Figure 1 and Figure 2 show the current level of complexity of the activities related to the standardization of the Internet of Things from different perspectives.
It has however to be noted that there is a growing awareness in the market and in the standardization arena with respect to the need of IoT standards convergence. Ongoing efforts in this perspective (e.g., recent actions to strengthen the collaboration among relevant SDOs involved in the horizontal/telecommunication dimension) are good premises of a simplification of this standards landscape in the medium term.
In this sense, in line with the goal and motivation of this deliverable, the experts participating in the AIOTI WG03 expect this landscaping exercise will also contribute to the promotion of the IoT standards convergence within the international community.

Appendix 1 (Section 5) provides the brief description of several SDO and Alliance initiatives shown in Figure 1 and Figure 2.

There are different technology trends to support IoT. Appendix 2 (Section 6) shows some of these technology trends.

3. IoT Open Source Software Initiatives Landscape

This section briefly introduces main IoT Open Source Software (OSS) initiatives that have a worldwide visibility and applicability and provides the global landscapes associated with these OSS initiatives. The "IoT Open Source Initiatives Landscape (Technology and Marketing Dimensions)" is a graphical representation that highlights the main activity (up to the day of generating this representation) of the open source initiatives in the area of IoT, according to the Business to Consumer (B2C) vs. Business to Business (B2B) (horizontal axis) and the Connectivity vs. Service & App (vertical axis) classifications. The dimensions of the landscape and the method used to project these OSS initiatives into the landscape shown in Figure 3 are the same ones as defined in Section 2.

Figure 3: IoT OSS Initiatives Landscape

It is important to be noticed that a projection of the OSS initiatives into vertical and horizontal industry domains, similar to the one shown in Figure 2, is not useful since the OSS initiatives are mainly focusing on the horizontal domain. Appendix 1 (Section 5) provides the brief description of several OSS initiatives shown in Figure 3.

4. Mapping SDO/Alliance/OSS/ Initiatives into Knowledge Areas

This section provides the mapping of each SDO/Alliance/OSS/Project initiative, mentioned in Section 2 and Section 3, into one or more of the following knowledge areas:

- Communication and Connectivity knowledge area*:*
  - It covers mainly specification of communication protocol layers, including PHY, MAC, NWK, Transport, Application layer, and their types, e.g., Wireless/Radio and Wire line; *it could also include management associated with the connectivity area*
- Integration/Interoperability knowledge area:
  - It covers mainly specification of common IoT features required to provide integration and interoperability
- Applications knowledge area:
  - It covers the support of the applications lifecycle including development tools/models, deployment and management; *including Analytics, application supporting tools and application domain specific activities*
- Infrastructure knowledge area:
  - It covers aspects related to the design, deployment, and management of computational platforms tailored to support IoT-based applications, attending requirements such as large-scale deployments, multi-tenant WSN, distributed computation and storage, and resource self-adaptation, among others
  - It includes topics such as software defined networks, cloud computing, Mobile Edge Computing (MEC), and fog computing
  - It considers the use cases and points-of-view of actors such as infrastructure service providers (e.g. network operators) and application service providers who use these infrastructures.
  - It could also include management associated with the infrastructure level
- IoT Architecture knowledge area:
  - It covers integrated/complete IoT specification solutions, including architecture descriptions
- Devices and sensor technology knowledge area:
  - It covers mainly device/sensor lifecycles, including operating systems, platforms, configuration management, *sensor/actuators virtualization etc.*
- Security and Privacy knowledge area:
  - It covers security and privacy topics

Figure 4 and Figure 5 show the mapping of the SDO/Alliance and OSS initiatives, respectively, into the knowledge areas described above. In Figure 4, the "Mapping of IoT SDOs/Alliances to Knowledge Areas" is a representation of the SDO and Alliance activities focusing on the different aspects of IoT, while in Figure 5, the "Mapping of IoT OSS initiatives to Knowledge Areas" is a representation of the OSS initiatives, focusing on the different aspects of IoT. This mapping representation focuses on the main SDO/Alliance and OSS initiatives up to the day of generating this representation.

The projection of these initiatives on these knowledge areas has been accomplished based on discussions among experts participating in both AIOTI WG03 and as well in the relevant initiatives and on the collected information presented in Appendix 1 (Section 5).

Figure 4: Mapping of IoT SDO and Alliance Initiatives into Knowledge Areas;
(*) A large number of initiatives shown in Section 2 that focus on vertical domains, can be mapped to the Application knowledge area

Figure 5: Mapping of IoT OSS Initiatives into Knowledge Areas

5. Appendix 1: IoT SDOs, Alliances and OSSs

This section provides a brief description of the SDO, Alliance and OSS initiatives shown in the landscapes figures included in Section 2.
This information has been provided by the AIOTI WG03 members on a volunteering basis, generated by filling in the templates shown in Section 5.1. Official confirmation/verification coming from the relevant initiatives is expected to be realized in the future.

5.1 SDO, Alliance, and OSS Initiatives Template for Information Collection

If the SDO/Alliance/OSS is a large initiative then the template should be applied for each of the Working Groups/Technical Committees that are focusing on IoT associated with that SDO/Alliance/OSS. The large initiatives identified at this stage are ITU, IEEE, IEC, 3GPP, ETSI, IETF.
If the required information is not available, please fill in "Unable to find information"

- Description: main objective and focus of the initiative
  Features: high level functionalities covered by the initiative
- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); for each criterion please select one or more options.
- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
  - Syntactical interoperability
  - Technical interoperability
  - Semantic interoperability
  - Organisational interoperability
- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); include details on whether an SDO/Alliance specified original protocols, or whether is using and integrating standards and protocols developed by other SDOs
- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative
- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
- Application area:
  - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
- Scope: mapping to knowledge areas of concerns in IoT.
  - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):
    - Communication and Connectivity knowledge area:
      - It covers mainly specification of communication protocol layers, e.g., PHY, MAC, NWK, Transport, Application layer, and their types, e.g., Wireless/Radio and Wire line; *it could also include management associated with the connectivity area*
    - Integration/Interoperability knowledge area:
      - It covers mainly specification of common IoT features required to provide integration and interoperability
    - Applications knowledge area:
      - It covers the support of the applications lifecycle including development tools/models, deployment and management; *including Analytics, application supporting tools and application domain specific activities*
    - Infrastructure knowledge area:
      - It covers aspects related to the design, deployment, and management of computational platforms tailored to support IoT-based applications,

attending requirements such as large-scale deployments, multi-tenant WSN, distributed computation and storage, and resource self-adaptation, among others
    - It includes topics such as software defined networks, cloud computing, Mobile Edge Computing (MEC), and fog computing
    - It considers the use cases and points-of-view of actors such as infrastructure service providers (e.g. network operators) and application service providers who use these infrastructures.
    - It could also include management associated with the infrastructure level
- IoT Architecture knowledge area:
    - It covers integrated/complete IoT specification solutions, including architecture descriptions
- Devices and sensor technology knowledge area:
    - It covers mainly device/sensor lifecycles, including operating systems, platforms, configuration management, *sensor/actuators virtualization etc.*
- Security and Privacy knowledge area:
    - It covers security and privacy topics

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy
- Specification Access: describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software

Table 1: OSS Readiness Criteria and Options

1. Community
    - Multiple individuals, no formal charter
    - Mostly one single organization
    - Multiple organizations
    - Formal consortium
2. Commitment
    - Mostly one committer
    - Multiple volunteer committers
    - Formally appointed committers from organizations
    - Dedicated committers from organizations
3. Road map:
    - Sporadic releases
    - Frequent but non planned releases (release when ready)
    - Planned releases
    - Formal road map
4. Alignment of ongoing Standards
    - Not aligned with SDO standards
    - OSS output is aligned with SDO specifications
5. Licensing
    - No license
    - Type of license
6. Portability
    - Only one target platform
    - Multiple platforms are possible but no developed
    - Multiple platforms are developed by project
    - Platform independent

Table 2: SDO/Alliance Readiness Criteria and Options

1. Adoption (users base)
   - No implementations
   - Reference implementations
   - Widely adopted in industry

2. Development Status
   - Under development
   - Approved with no planned revisions
   - Approved with planned revisions
3. Compliance
   - Not managed
   - Having compliance testing process (include test suites, method, etc.)
   - Formal certification process
4. Openness
   - Very restrictive membership and closed to few entities
   - Restrictive membership procedure
   - Open by formal membership
   - Open to public
5. Ratification process (how the standard is being approved?)
   - Closed process done by members only with no consultation from external parties
   - Done by members and open for consultation from external parties
   - Open process for all parties interested in the ratification

More details on interoperability levels are provided below:

- **Technical Interoperability**: is usually associated with hardware/software components, systems and platforms that enable machine-to-machine communication to take place. This kind of interoperability is often centred on (communication) protocols and the infrastructure needed for those protocols to operate.
- **Syntactical Interoperability**: is usually associated with data formats. Certainly, the messages transferred by communication protocols need to have a well-defined syntax and encoding, even if it is only in the form of bit-tables. However, many protocols carry data or content, and this can be represented using high-level syntaxes such as HTML or XML
- **Semantic Interoperability**: is usually associated with the meaning of content and concerns the human rather than machine interpretation of the content. Thus, interoperability on this level means that there is a common understanding between people of the meaning of the content (information) being exchanged.
- **Organizational Interoperability**, as the name implies, is the ability of organizations to effectively communicate and transfer (meaningful) data (information) even though they may be using a variety of different information systems over widely different infrastructures, possibly across different geographic regions and cultures. Organizational interoperability depends on successful technical, syntactical and semantic interoperability.

5.2 IoT SDO/Alliance Initiatives

This section provides a brief description of the SDO and Alliance initiatives mentioned in Section 2. These brief descriptions are following and are based on the SDO and Alliance template described in Section 5.1.

The official URLs of each of these initiatives can be found via Table 3, Table 4 and Table 5.

Table 3: SDO/Alliance initiatives and their Official URLs: Part 1

Initiative	URL
3GPP (3rd Generation Partnership Project)	http://www.3gpp.org/
ACEA (European Automobile manufacturing Association):	http://www.acea.be/
AEF (Agricultural Industry Electronics Foundation)	http://www.aef-online.org/
AIOTI (Alliance for Internet of Things Innovation)	http://www.aioti.eu/
Allseen Alliance	https://allseenalliance.org/
ASHRAE	https://www.ashrae.org/
AVNU	http://avnu.org/
Bluetooth	http://www.bluetooth.com/
Broadband Forum	https://www.broadband-forum.org/
Calypso	https://www.calypsonet-asso.org/
C2C-CC (Car-2-Car Communication Consortium)	https://www.car-2-car.org/
CCC (Car Connectivity Consortium)	http://carconnectivity.org/
CC-Link	http://www.cclinkamerica.org
CEN (European Committee for Standardization)	https://www.cen.eu/
CENELEC (European Committee for Electrotechnical Standardization)	http://www.cenelec.eu/
CIA (CAN IN Automation)	http://www.can-cia.org/
CIIAII (China Integration and Innovation Alliance of Internet and Industry)	http://www.ciiaii.org.cn/
CLEPA	http://www.clepa.eu/working-groups/technical-regulations-tr/
Continua: Health Alliance	http://www.continuaalliance.org/
DICOM (Digital Imaging and Communications in Medicine)	http://dicom.nema.org/
easyway	https://www.easyway-its.eu/
eCl@ss	http://www.eclass.de/
ERTICO - ITS Europe	http://ertico.com/
ETSI (European Telecommunications Standards Institute)	http://www.etsi.org/
Enocean Alliance	https://www.enocean-alliance.org/

Table 4: SDO/Alliance initiatives and their Official URLs: Part 2

Initiative	URL
GSMA	http://www.gsma.com/
HGI (Home Gateway Initiative)	http://www.homegatewayinitiative.org/
HL7 International (Health Level 7)	http://www.hl7.org/
HYPER/CAT	http://www.hypercat.io/
IEC (International Electrotechnical Commission)	http://www.iec.ch/
IEEE (Institute of Electrical and Electronics Engineers)	http://www.ieee.org/
IEEE 802 LAN/MAN Standards Committee	http://www.ieee802.org/
IEEE P2413:	http://grouper.ieee.org/groups/2413/
IETF (Internet Engineering Task Force)	http://www.ietf.org/
IHE (Integrating the Healthcare Enterprise)	http://www.ihe.net/
IIC (Industrial Internet Consortium)	http://www.industrialinternetconsortium.org/
IPSO (Internet Protocol for Smart Object)	http://www.ipso-alliance.org/
IRTF (Internet Research Task Force)	http://www.3gpp.org/
IO-Link	http://www.io-link.com/
IoT Security Foundation	https://www.iotsecurityfoundation.org/
IPEN (Internet Privacy Engineering Network)	https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/IPEN
ISA (International Society of Automation)	https://www.isa.org/
ISO (International Organization for Standardization)	http://www.iso.org/
ISO/IEC JTC 1	http://www.iso.org/iso/jtc1_home.html
ITU (International Telecommunication Union)	http://www.itu.int/
The KNX Association	http://www.knx.org/
LoRa Alliance	https://www.lora-alliance.org/

Table 5: SDO/Alliance initiatives and their Official URLs: Part 3

Initiative	URL
OASIS	https://www.oasis-open.org/
OAA(Open Automotive Alliance)	http://www.openautoalliance.net
ODVA	https://www.odva.org/
OGC (Open Geospatial Consortium)	http://www.opengeospatial.org/
OIC (Open Interconnect Consortium)	http://openinterconnect.org/
OMA (Open Mobile Alliance)	http://openmobilealliance.org/
The ULE (Ultra Low Energy) Alliance	http://www.ulealliance.org/
OMG (Object Management Group)	http://www.omg.org/
OneM2M	http://www.onem2m.org/
OPC (Open Platform Communications) Foundation	https://opcfoundation.org/
The Open Group	http://www.opengroup.org/
OSGi Alliance	http://www.osgi.org/
PI (Profibus - Profinet) International	http://www.profibus.com/
Platform Industrie 4.0	http://www.plattform-i40.de/
SAE International	http://www.sae.org/
SGIP (Smart Grid Interoperability Panel)	http://sgip.org/
Thread group	http://threadgroup.org/
UPnP (Universal Plug and Play)	http://upnp.org/
W3C (World Wide Web Consortium)	http://www.w3.org/
Weightless	http://www.weightless.org/
Wi-Fi Alliance	http://www.wi-fi.org/
Wireless World Research Forum	http://www.wwrf.ch/
The ZigBee Alliance	http://www.zigbee.org/
XMPP	http://xmpp.org/

5.2.1 3GPP (3rd Generation Partnership Project)

- Description:

  (adapted /shortened from www.3gpp.org)

  The project covers cellular telecommunications network technologies, including radio access, the core transport network, and service capabilities - including work on codecs, security, quality of service - and thus provides complete system specifications. 3GPP specifications and studies are contribution-driven, by Member companies (originating from its Organizational Partners), in Working Groups and at the Technical Specification Group level.

  The Four Technical Specification Groups (TSG) in 3GPP are;

  - Radio Access Networks (RAN),
  - Service & Systems Aspects (SA),
  - Core Network & Terminals (CT) and
  - GSM EDGE Radio Access Networks (GERAN).

  The last meeting of a cycle of Plenary meetings is TSG SA, which also has responsibility for the overall coordination of work and for the monitoring of its progress.

The 3GPP technologies from these groups are constantly evolving through Generations of commercial cellular / mobile systems. Since the completion of the first LTE and the Evolved Packet Core specifications, 3GPP has become the focal point for mobile systems beyond 3G.

Backward Compatibility

The major focus for all 3GPP Releases is to make the system backwards and forwards compatible where-ever possible, to ensure that the operation of user equipment is un-interrupted. A good current example of this principle has been the priority placed in the working groups on backward compatibility between LTE and LTE-Advanced, so that an LTE-A terminal can work in an LTE cell and an LTE terminal works in the LTE-A cell.

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.
  1. Adoption (users base)
     - Widely adopted in industry
  2. Development Status
     - Approved with planned revisions
  3. Compliance
     - Having compliance testing process (include test suites, method, etc.)
     - Formal certification process
  4. Openness
     - Open by formal membership
     - Open to public
  5. Ratification process (how the standard is being approved?)
     - Done by members and open for consultation from external parties

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
  - Technical interoperability
  - Organisational interoperability

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs

  As referred above 3GPP covers cellular telecommunications network technologies, including radio access, the core transport network, and service capabilities - including work on codecs, security, quality of service - and thus provides complete system

specifications

3GPP specifications also provide hooks for non-radio access to the core network, and for interworking with Wi-Fi networks.

In particular, 3GPP specifications are taking into account IoT needs, namely know through a strong focus on the CIoT (Cellular IoT) and the support of Vehicular communications (LTE-Vx).

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative

  The 3rd Generation Partnership Project (3GPP) unites [Seven] telecommunications standard development organizations from Europe, China, India, Japan Korea and US (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), known as "Organizational Partners"

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
  - 3GPP provides network connectivity along the entire horizontal axis and mainly in vertical axis part under the horizontal axis.

- Application area:
  - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2.
    - 3GPP is not chartered to focus on a particular vertical industry. It provides standardized network layer technologies that are applicable to the various industry domains.

- Scope: mapping to knowledge areas of concerns in IoT.
  - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):
    - Communication and Connectivity knowledge area
    - Integration/Interoperability knowledge area
    - Infrastructure knowledge area

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy:
  http://www.3gpp.org/about-3gpp/legal-matters
  http://www.3gpp.org/ftp/Information/Working_Procedures/3GPP_WP.htm#Article_55
  http://www.3gpp.org/ftp/Inbox/2008_web_files/3gppagre.pdf

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software
  - Specification open 3GPP web site – free to access for all.

5.2.2 AVNU Alliance

- Description:
  - The AVnu Alliance is a community creating an interoperable ecosystem servicing the precise timing and low latency requirements of diverse applications using open standards through certification. www.avnu.org

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.
  1. Adoption (users base)
     - Widely adopted in industry
  2. Development Status
     - Approved with planned revisions
  3. Compliance
     - Formal certification process
  4. Openness
     - Open by formal membership
  5. Ratification process (how the standard is being approved?)
     - Done by members and open for consultation from external parties

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
  - Technical interoperability
- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs
  - Certification procedures based on Open standards (IEEE 802.1TSN, 802.1 series, IEEE 1588, IETF DetNet…)

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative: Leader in
  - Automotive
  - Industrial automation
  - Audio / video

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
  - Automotive
  - Industrial automation
  - Audio / video

- Application area:
  - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2.

    - Smart manufacturing
    - Automotive
    - Audi / Video

- Scope: mapping to knowledge areas of concerns in IoT.
  - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):
    - Communication and Connectivity knowledge area:
    - Integration/Interoperability knowledge area:
    - Infrastructure knowledge area:
    - IoT Architecture knowledge area:
    - Devices and sensor technology knowledge area:
    - Security and Privacy knowledge area:

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy
    - FRAND (http://avnu.org/wp-content/uploads/2014/05/AVnu-Alliance-IPR-Policy.pdf)

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software
    - Open to everyone with a fee.

5.2.3 BBF (Broadband Forum): Broadband User Services (BUS) Work Area

- Description:
    - The BBF Work Area: Broadband User Services (BUS) work area is a new area that has been created after the BBF restructuring that took place in 2015. Please note that previously, the Working Group that focused the most on IoT related specifications was the BroadbandHome WG, which was dismissed at the moment that the BUS Work Area has been created. The BroadbandHome WG provided the TR-069 that specifies the CPE WAN Management Protocol, intended for communication between a CPE and Auto-Configuration Server (ACS).
    - More details on this area can be found via: https://www.broadband-forum.org/technical/technicalwip.php#WABUS. The following text has been copied from the provided URL:
        - Mission Statement:
            - The Broadband User Services Work Area provides the broadband industry with technical specifications, implementation guides, reference implementations, test plans, and marketing white papers for the deployment, management, and consumption of services by the broadband end user. This Work Area represents the end user perspective when incorporating into the Broadband Forum architecture.
        - Business Impact:
            - The Broadband User Services Work Area develops specifications and publications to create a new kind of the Broadband experience for the end user and provides new means for service providers and application developers to monetize the broadband user's connection. This ranges from on-demand performance assured business and entertainment services, IoT services related to energy, security, environment, etc. to user control of what can become the data center in the home and small business managed and control with zero- touch diagnostics. All of which opens up large markets and profitable business models.
        - Scope:
            - Develop and evolve the TR-069 CPE WAN Management Protocol and a Universal Service Platform (USP) to cover existing use cases, machine-to-machine/IoT use cases, and the virtualization of broadband user services, prioritized by their potential business value
            - Develop and specify new information models to broaden the range of for which TR-069 and USP can be used
            - Develop requirements for broadband user devices and associated software
            - Develop test plans and training programs for Work Area protocols and requirements
            - Develop marketing white papers that supplement Work Area protocols and requirements

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.
    1. Adoption (users base)
        - Reference implementations
        - Widely adopted in industry

    2. Development Status
        - Approved with planned revisions

3. Compliance
    - Having compliance testing process (include test suites, method, etc.)
    - Formal certification process
4. Openness
    - Open by formal membership
    - Open to public
5. Ratification process (how the standard is being approved?)
    - Closed process done by members only with no consultation from external parties

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative
    - Syntactical interoperability
    - Technical interoperability

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs
    - The BBF BUS Work Area will develop and evolve the TR-069 CPE WAN Management Protocol (CWMP) and a Universal Service Platform (USP) to cover existing use cases, machine-to-machine/IoT use cases, and the virtualization of broadband user services, prioritized by their potential business value
      The produced documents related to TR-069 are, listed below. These can be downloaded via: https://www.broadband-forum.org/technical/trlist.php:
        - TR-069: Ammendment 1: CPE WAN Management Protocol (December 2006)
        - TR-069: Ammendment 2: CPE WAN Management Protocol v1.1 (December 2007)
        - TR-069: Ammendment 3: CPE WAN Management Protocol (November 2010)
        - TR-069: Ammendment 4: CPE WAN Management Protocol (July 2011)
        - TR-069: Ammendment 5: CPE WAN Management Protocol (November 2013)
        - TR-330: TR-069 UPnP DM Proxy Management Guidelines
        - TR-181: Device Data Model for TR-069 (February 2010)
        - TR-181 Device Data Model for TR-069 Issue 2, (May 2010)
        - TR-181 Device Data Model for TR-069 Issue 2, Amendment 2 (February 2011)
        - TR-181 Device Data Model for TR-069, Issue 2, Amendment 5 (May 2012)
        - TR-181 Device Data Model for TR-069 Issue 2 Amendment 6 (November 2012)
        - TR-181 Device Data Model for TR-069 Issue 2 Amendment 7 (November 2013)
        - TR-181 Device Data Model for TR-069 Issue 2 Amendment 8 (september 2014
        - TR-154: TR-069 Data Model XML User Guide (March 2012)
        - TR-142: Framework for TR-069 enabled PON devices (March 2008)
        - TR-142: Framework for TR-069 enabled PON devices Issue 2 (February 2010)
        - TR-140: TR-069 Data Model for Storage Service Enabled Devices, Amendment 1 (April 2010)
        - TR-140: TR-069 Data Model for Storage Service Enabled Devices. Issue 1.1: (December 2007)
        - TR-135: Data Model for a TR-069 Enabled STB (December 2007)
        - TR-106: Amendment 1: Data Model Template for TR-069-Enabled Devices (November 2006)
        - TR-106: DSLHomeTM Data Model Template for TR-069 Enabled Devices (September 2006)
        - TR-098: Internet Gateway Device Data Model for TR-069 (December 2006)
        - TR-157: Component Objects for CWMP (March 2009)
    - For more details on the CWMP (CPE WAN Management Protocol) protocol, please visit:
      https://www.broadband-forum.org/cwmp.php
      https://www.broadband-forum.org/cwmptools.php

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative: BUS is a BBF Work Area.

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
    - Market domain: Closer to the Consumer market edge of the vertical axis.
    - Technical domain: Located on the horizontal axis, to show that it is equally focusing on connectivity and service&applications.

- Application area: whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
    - The BUS Work Area is mainly focusing on horizontal industries. It needs to be emphasized that the CWMP protocol specified in TR-069 is widely applied/used in the Home/Building area.

- Scope: mapping to knowledge areas of concerns in IoT.
    - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):
        - Communication and Connectivity knowledge area*:*
            - covers mainly the Application layer
        - Infrastructure knowledge area:
            - Covers aspects related to the design, deployment, and management of computational platforms tailored to support IoT-based applications, attending requirements such as large-scale deployments, multi-tenant WSN, distributed computation and storage, and resource self-adaptation, among others

- IPR Policy Available:
    - Information regarding the used BBF IPR policy can be found via: https://www.broadband-forum.org/technical/ipdeclarations.php.

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software
    - For members:
        - Access of published and non-published specifications for members and non-members is open and free of payment.
    - For non-members:
        - Access of published specifications is open and free of payment
        - Access of non-published specifications is not possible.
        - Other SDO/Alliances/OSS initiative can access non-published documents via written liaisons

5.2.4 ETSI (European Telecommunications Standards Institute)

This section provides a brief description of the ETSI SDO initiative and its IoT related Technical Committees (TCs) and Industry Specification Groups (ISGs).

ETSI initiative

- Description:
  ETSI, the European Telecommunications Standards Institute, produces globally-applicable standards for Information and Communications Technologies (ICT), including

fixed, mobile, radio, converged, broadcast and Internet technologies. Our standards enable the technologies on which business and society rely. For example, our standards for GSM™, DECT™, Smart Cards and electronic signatures have helped to revolutionize modern life all over the world.

ETSI are officially recognized by the European Union as a European Standards Organization.

ETSI are a not-for-profit organization with more than 800 member organizations worldwide, drawn from 64 countries and five continents. Members include the world's leading companies and innovative R&D organizations.

ETSI are at the forefront of emerging technologies. We address the technical issues which will drive the economy of the future and improve life for the next generation.

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.

    1. Adoption (users base)
        Widely adopted in industry
    2. Development Status
        Depends on group and specification
    3. Compliance
        Having compliance testing process (include test suites, method, etc.)
    4. Openness
        Open to public – most groups some only open to members

    5. Ratification process (how the standard is being approved?)
        Done by members and open for consultation from external parties

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
    - Organisational interoperability

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs
    - Depends on specification

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
    - Multiple domains

- Application area:
    - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is

focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
    - Different specifications cover different areas.

- Scope: mapping to knowledge areas of concerns in IoT.
  - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):
    - Different specifications cover different areas

    - Communication and Connectivity knowledge area:
    - Integration/Interoperability knowledge area:
    - Applications knowledge area:
    - Infrastructure knowledge area:
    - IoT Architecture knowledge area:
    - Devices and sensor technology knowledge area:
    - Security and Privacy knowledge area:

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy
  - FRAND – ETSI IPR policy - http://www.etsi.org/about/how-we-work/intellectual-property-rights-iprs

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software
  - Specification open ETSI web site – free to access for all.

ETSI TC ATTM

- Description:
  The scope of Technical Committee (TC) ATTM addresses Access, Terminals, Transmission and Multiplexing including all aspects within the ETSI scope covering cabling, installations, signal transmission, multiplexing and other forms of signal treatment up to digitalization in private and public domain, excluding those aspects that relate to Hybrid Fibre-Coaxial cable networks which are covered by TC Cable. A close cooperation and collaboration will be maintained between TC Cable and TC ATTM in areas of mutual interest.

  TC ATTM closely collaborates with the Technical Body(ies) (TB) responsible for Communications Networking and Services and the exact border line between the activities will be adapted to the members' needs. Signalling protocols are excluded from ATTM, except for identified technologies like POTS interaction between terminals and networks, e.g. seizing, releasing the line, dialling and calling.

  TC ATTM studies the applicability and implementation of ISO / IEC / CENELEC as well as ITU / ETSI drafts and deliverables related to the Residential, Professional, Industrial and Operators' premises including communication equipment. The activities cover all relevant influences from other organizations, coordination, convergence and

standardization of the various initiatives and an efficient liaising effort with relevant bodies.

TC ATTM primarily focuses on:
Attracting and enhancing expertise with the objective to develop and maintain ETSI deliverables on all aspects of infrastructures and transmission within its scope
Where requested by another ETSI TB, support their work on infrastructures and transmission aspects
Access network aspects within its scope

Within its scope, TC ATTM addresses the specific technology, equipment, installations and regulatory aspects of the physical layer, e.g. of:
Transmission issues of interfaces
Frequency management on the non-radio Communication Infrastructures
Analogue and digital presented Communication interfaces of balanced wired (twisted pair), and unbalanced wires (coaxial) and optical fibre Infrastructures
Interfaces based on new technologies as far as they are relevant for Communication Infrastructures
Point-to-point and point-to-multipoint radio systems and infrastructures used for the fixed service (core and access networks), covering all equipment aspects including antenna parameters
Transmission related aspects of network architecture(s) (including protection issues)
Specification of the transmission functions and performance of the network elements such as transmission paths, path elements, sections, systems, functional entities, antenna, cable and optical fibre

Within its scope, TC ATTM will:

- advise the relevant ESO bodies on transmission aspects of service requirements
- work on end to end transmission over networks in support of customer's applications
- support the development of appropriate interfaces to network based services always in collaboration with relevant TB

Additionally each one of the ATTM WG in their area of activity, under the leadership of TC ATTM will contribute to the promotion at a global level of the existing ETSI deliverables to the development of a consistent approach to standardization of emerging technologies and services with a view towards producing global standards.

TS 105 XXX Networks connecting digital multi-services in cities.
TS 105 174 Series Eco-efficient Engineering in order to support deployment of eco-efficient networks and sites.
ES 205 200 Series Global Key Performance Indicators - to provide ICT users with tools to monitor their eco-efficiency and energy management in compliance with Kyoto Protocol on climate change and reduction of greenhouse gas emissions.
TS 105 175-1 Engineering of plastic optical fibre networks within building.
EN 305 XXX Eco-efficient End of Life - to provide ICT suppliers and users with tools to implement "Green" tools (indicators, recognized Green levels) to monitor waste processing of ICT equipment in compliance with Kyoto Protocol on climate change and reduction of greenhouse gas emissions.

ES Planned Eco-efficient End of Life - to provide ICT suppliers and users with tools to implement "Green" tools (indicators, recognized Green levels) to monitor sustainability of broadband solutions.

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.

1. Adoption (users base)
   Widely adopted in industry

2. Development Status
   Depends on specification, some published others under development
3. Compliance
   Having compliance testing process (include test suites, method, etc.)
4. Openness
   Open to public – most groups some only open to members

5. Ratification process (how the standard is being approved?)
   Done by members and open for consultation from external parties

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
  - Organisational interoperability.

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs
  - Depends on specification

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative
  - Not relevant

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
  - Multiple domains

- Application area:
  - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
    - Different specifications cover different areas. Smart City focus in some specifications

- Scope: mapping to knowledge areas of concerns in IoT.
  - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):

- Communication and Connectivity knowledge area:
- Integration/Interoperability knowledge area:
- Applications knowledge area:
- Infrastructure knowledge area:
- IoT Architecture knowledge area:
- Devices and sensor technology knowledge area:
- Security and Privacy knowledge area:

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy
  - FRAND – ETSI IPR policy - http://www.etsi.org/about/how-we-work/intellectual-property-rights-iprs

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software
  - Specification open ETSI web site – free to access for all.

ETSI TC CYBER

- Description:

Responsibility:

The main responsibilities of ETSI TC CYBER are:
To act as the ETSI centre of expertise in the area of Cyber Security
Advise other ETSI TCs and ISGs with the development of Cyber Security requirements
To develop and maintain the Standards, Specifications and other deliverables to support the development and implementation of Cyber Security standardization within ETSI
To collect and specify Cyber Security requirements from relevant stakeholders
To identify gaps where existing standards do not fulfil the requirements and provide specifications and standards to fill these gaps, without duplication of work in other ETSI committees and partnership projects
To ensure that appropriate Standards are developed within ETSI in order to meet these requirements
To perform identified work as sub-contracted from ETSI Projects and ETSI Partnership Projects
To coordinate work in ETSI with external groups such as Cyber Security Coordination group in CEN CENELEC and ENISA
To answer to policy requests related to Cyber Security, and security in broad sense in the ICT sector.

Areas of activity

The activities of TC CYBER will be performed in close co-operation with relevant standards activities within and outside ETSI.
The activities of ETSI TC CYBER include the following broad areas:
Cyber Security
Security of infrastructures, devices, services and protocols
Security advice, guidance and operational security requirements to users, manufacturers and network and infrastructure operators
Security tools and techniques to ensure security

Creation of security specifications and alignment with work done in other TCs.

Organisation and working methods

TC CYBER shall work in accordance with the normal rules as given in the ETSI Directives and, in particular, the Technical Working Procedures.

The tasks described above will require liaisons with relevant bodies within ETSI as well as outside ETSI according to the rules prescribed by the ETSI Directives.

Internal to ETSI:

ETSI TCs that have a requirement for Security in their work. Examples are LI, SAGE, and SmartM2M. It is recognised that Security is a vertical activity and undertaken within groups, whilst TC CYBER may provide advice, guidance and horizontal coordination

ETSI ISGs that have a requirement for security in their work

External to ETSI:

Coordination with European, National and International standards organisations, as well as other bodies such as ENISA, 3GPP, oneM2M, and Professional organisations etc.

Participation

Participation in TC CYBER is open to all ETSI members in accordance with the Technical Working Procedures. Observers and non-members may participate at the discretion of the Chairman in-line with clause 1.4 of the Technical Working Procedures..

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.
  1. Adoption (users base)
     Widely adopted in industry
  2. Development Status
     Depends on specification, some published others under development
  3. Compliance
     Having compliance testing process (include test suites, method, etc.)
  4. Openness
     Open to public – most groups some only open to members

  5. Ratification process (how the standard is being approved?)
     Done by members and open for consultation from external parties

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
  - Organisational interoperability

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs
  - Depends on specification

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative
    - Not relevant

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
    - Multiple domains

- Application area:
    - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
        - Different specifications cover different areas. Smart City focus in some specifications

- Scope: mapping to knowledge areas of concerns in IoT.
    - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):
        - Security and Privacy knowledge area:

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy
    - FRAND – ETSI IPR policy - http://www.etsi.org/about/how-we-work/intellectual-property-rights-iprs

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software
    - Specification open ETSI web site – free to access for all.

ETSI TC DECT

- Description:
    - DECT Ultra Low Energy (ULE) is a technology based on DECT, intended for Machine-to-Machine communications such as Home and Industrial automation. The main characteristics of the technology are ultra low power consumption and wider coverage
    - The technology is suitable for sensors, alarms, Machine-to-Machine (M2M) applications, utility meters and industrial automation.
    - ETSI TC DECT has the overall responsibility over DECT and ULE technologies.

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.

    1. Adoption (users base)
        - Reference implementations and first commercial products of Phase 1 (see standards)
    2. Development Status
        - Approved with planned revisions

3. Compliance
    - Formal certification process (managed by the ULE-Alliance)
4. Openness
    - Open to public
5. Ratification process (how the standard is being approved?)
    - Done by members and open for consultation from external parties

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
    - Complete technical interoperability from Physical layer to application layer

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs
    - TC DECT is the original developing organization of ULE technology .
        - Other organizations may provide application protocols
    - Standards:
        - Main Specifications: ETSI TS 102 939-1 (DECT ULE phase 1) and ETSI TS 102 939-2 (DECT ULE phase 2)
        - ULE functions are added to the DECT Common Interface specification (ETSI EN 300 175 parts 1 to 8) where technical details organized by layers can be found.
        - ULE uses its own security model based on CCM (algorithms and procedures defined in EN 300 175-7)
        - From radio compliance perspective, ULE re-uses the Harmonised ENs of DECT (EN 301 406 and EN 301 908-10)
        - Under developing:
            - Repeaters
        - ULE-Alliance has developed an own application protocol (the FUN) , however ULE technology is open to any other higher layer.

- Supporting organizations
    - Open to ETSI membership
    - Active participants from industry vendors and operators
    - An industry Alliance, the ULE-Alliance is in charge of promoting the technology and driving the certification program.

- Domain:
    - position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
        - Both consumer (home automation) and industrial markets addressed (industry automation)
        - both horizontal and domain specific. Strong in Retail and Operators business.
        - Technical domain :connectivity / communications and Networking

- Application area:
    - Home / building (Smart living)

- Smart cities
- Energy
- Healthcare (Smart living)
- Wearables
- Smart manufacturing/ industry automation

- Scope: mapping to knowledge areas of concerns in IoT.
  - The primary knowledge areas is Communication and Connectivity knowledge area:
  - An additional knowledge areas is Devices and sensor technology knowledge area:

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy
  - FRAND

- Specification Access: ETSI specifications are publicly available

ETSI TC ERM

- Description:

Responsibility

The Horizontal TC (EMC and Radio spectrum matters) has the primary responsibility for:
ETSI deliverables (in whole or in part) dealing with EMC;
ETSI deliverables (in whole or in part) dealing with radio spectrum parameters concerned with inter-system characteristics;
co-ordination of ETSI positions on the efficient use of the radio spectrum and spectrum allocations;

Such ETSI deliverables may include harmonised standards intended to be used for regulatory purposes.
co-ordination of ETSI positions on the efficient use of the radio spectrum and spectrum allocations;
a range of ETSI deliverables dealing with radio equipment and systems where they are not undertaken by other ETSI groups, the deliverables may include product and harmonised (regulatory) standards concerned with inter-system characteristics;

The TC (EMC and Radio Spectrum Matters) is the formal interface in respect of radio spectrum and electromagnetic compatibility between ETSI and EC/EFTA, including RSCOM and RSPG; other bodies in the radio and EMC field, notably the CEPT ECC, relevant CEN and CENELEC committees, EUROCAE and EBU, relevant ICAO and ITU groups; IEC and CISPR.

Areas of activity

The activities of TC-ERM (EMC and Radio Spectrum Matters) falls into two broad areas of work, horizontal across ETSI and vertical project orientated

activities. All TC-ERM activities have a common theme of electromagnetic and/or radio spectrum compatibility.

Horizontal Activities

Studies of the EMC and radio parameters and their methods of measurement - taking due account of the work in the international community and specifically IEC;
Preparation of ETSI deliverables as required by ETSI members or those to support mandated work from the EC/EFTA in support of EU Directives or as requested by CEPT ECC;
Preparation of ETSI deliverables including harmonised standards used to describe the electromagnetic and/or radio environment;
Co-ordination of ETSI positions on the efficient use of the radio spectrum and spectrum allocations and the administration of the MoU between CEPT ECC and ETSI. These activities will be carried out in close co-operation with relevant ETSI Technical Bodies;
TC-ERM (EMC and Radio Spectrum Matters) also provides ETSI with a centre of technical expertise in the radio and EMC fields, able to offer advice to ETSI Technical Bodies, the ETSI Board, and the ETSI General Assembly.

Vertical Project Oriented Activities

Following from the restructuring of the work of TC-RES, TC-ERM is the parent body for project oriented (vertical) radio equipment and system standardisation activities. TC-ERM, via designated Task Groups, provides ETSI with a range of deliverables for sundry radio equipment and systems. TC‑ERM is also designated as the host radio project activities that have entered their maintenance phase.

A non exhaustive activity list of radio standardisation activities includes:- Aeronautical - Automotive - Broadcast and broadcast ancillary equipment – CDMA for private and public access mobile radio - Short range devices including generic devices, avalanche beacons, inductive data communications, RF identification devices - Intelligent transport systems including road transport & traffic telematics - Maritime - Private mobile radio (PMR) including digital mobile radio - Measurement Uncertainty - Radio site engineering - Wireless medical devices - Wideband data systems - Ultra wideband (UWB) including automotive radar and short range communication plus Harmonised standards for the IMT-2000 family (joint with MSG).

Organisation and working methods within the Committee

TC-ERM has organised itself following the principles of ‘delayering’ in accordance with ETSI Technical Working Procedures by the creation of two Working Groups; ERM-RM (Radio Matters) and ERM-EMC (Electromagnetic Compatibility) together with a range of project oriented Task Groups, as indicated above, designated to undertake a specific task and when the task is completed to enter a dormant mode or be disbanded as appropriate.

For work items of a radio spectrum and/or regulatory nature subject to the CEPT/ETSI MoU, joint groups with CEPT ECC and its working groups are planned if needed to facilitate the necessary coordination.

Co-operation with CENELEC - for EMC work items and specifically mandated activities, joint groups will be established where appropriate. Similarly in the maritime sector joint groups with the IEC TC80 are planned.

EN 303 204 Radio equipment to be used in the 870 MHz to 876 MHz frequency range with power levels ranging up to 500 mW.
EN 300 220 Radio equipment to be used in the 25 MHz to 1 000 MHz frequency range with power levels ranging up to 500 mW:
SSN is active in a number of Smart City application domains (e.g. Smart Street Lighting) and device connections via RF Mesh infrastructure to back-office applications meet many Smart City requirements as well as Smart Metering. Capacity available is sufficient to enable Smart City infrastructure to be shared by multiple applications and provide capacity for the future growth as Smart City services develop.
Emerging interoperability specifications (e.g. Wi-SUN) are consistent with EN 303 204 as well as EN 300 220 - continues to be principal underlying spectrum access standard for licence exempt devices.
DTR/ERM-TGDMR-340 Technical Report on Smart Grid Systems and Other Radio Systems suitable for Utility Operations and their long-term spectrum requirements.

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.
    1. Adoption (users base)
        Widely adopted in industry
    2. Development Status
        Depends on specification, some published others under development
    3. Compliance
        Having compliance testing process (include test suites, method, etc.)
    4. Openness
        Open to public – most groups some only open to members

    5. Ratification process (how the standard is being approved?)
        Done by members and open for consultation from external parties

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
    - Organisational interoperability.

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs
    - Depends on specification

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative

    - Not relevant

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
    - Multiple domains

- Application area:
    - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
        - Different specifications cover different areas. Smart City focus in some specifications

- Scope: mapping to knowledge areas of concerns in IoT.
    - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):
        - Communication and Connectivity knowledge area:
        - Integration/Interoperability knowledge area:
        - Applications knowledge area:
        - Infrastructure knowledge area:
        - IoT Architecture knowledge area:
        - Devices and sensor technology knowledge area:
        - Security and Privacy knowledge area:

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy
    - FRAND – ETSI IPR policy - http://www.etsi.org/about/how-we-work/intellectual-property-rights-iprs

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software
    - Specification open ETSI web site – free to access for all.

ETSI TC HF (Human Factors)

- Description:
  The Human Factors committee is the technical body within ETSI responsible for Human Factors issues in all areas of Information and Communications Technology (ICT). It produces standards, guidelines and reports that set the criteria necessary to build optimum usability into the emerging digital networked economy (DNE).

  The HF committee co-operates with other groups within ETSI and outside to assist them to produce standards, or other deliverables, which are in accordance with good Human Factors practice. Within ETSI it has a special responsibility for "Design for All" addressing the needs of all users, including young children, seniors and disabled people.

  Human Factors is the scientific application of knowledge about human capacities and limitations

in order to make products, systems, services and environments effective, efficient and easy for everyone to use. It is a key factor for the commercial success of any ICT product or service in the digital networked economy.

New work area resulting from discussion with:
EDF (European Disability Forum),
European Blind Union,
ANEC,
European Age Platform.

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.

  1. Adoption (users base)
     Widely adopted in industry
  2. Development Status
     Depends on specification, some published others under development
  3. Compliance
     Having compliance testing process (include test suites, method, etc.)
  4. Openness
     Open to public

  5. Ratification process (how the standard is being approved?)
     Done by members and open for consultation from external parties

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
  - Organisational interoperability.

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs
  - Depends on specification

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative
  - Not relevant

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
  - Multiple domains

- Application area:
  - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
    - Focus on access for all

- Scope: mapping to knowledge areas of concerns in IoT.
  - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):
    - Access for all – human interaction

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy
    - FRAND – ETSI IPR policy - http://www.etsi.org/about/how-we-work/intellectual-property-rights-iprs

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software
    - Specification open ETSI web site – free to access for all.

ETSI TC ITS (Intelligent Transport Systems)

- Description:

Responsibility

Development and maintenance of Standards, Specifications and other deliverables to support the development and implementation of ITS Service provision across the network, for transport networks, vehicles and transport users, including interface aspects and multiple modes of transport and interoperability between systems, but not including ITS application standards, radio matters, and EMC.

Scope includes communication media, and associated physical layer, transport layer, network layer, security, lawful intercept and the provision of generic web services

Areas of Activity

The activities of TC ITS will be performed in close co-operation with relevant standards activities within and outside ETSI. The activities of TC ITS include the:

To work in close liaison with other SDOs, particularly those responsible for providing application standards, to ensure seamless access and interoperability of Standards to support ITS service provision

To act as a focal point for initial standardisation and awareness of standardisation requirements and expertise for European development and provision of ITS services.

To act as a focal point and centre of expertise and excellence within ETSI in respect of Intelligent Transport Systems and coordinate with other ETSI committees, and where appropriate to represent ETSI in respect of ITS

To liaise and cooperate with the European Commission and ITS trade organisations in respect of enabling ITS service provision, quality assurance and certification

To liaise to ETSI ERM for ERM related spectrum matters and EMC, This includes that ERM and its TG's remain as the focal point for spectrum related liaisons to ECC.

To organize regular meetings/workshops with appropriate stakeholders.

To establish external relationships (and joint working groups) where and whenever needed, including co-operation with 3GPP, CEN, CENELEC, ISO, ITU etc. Formal relationships will be established using the normal processes via the ETSI Secretariat (NIM/Partnerships).

The technical standardization work of the following bodies is explicitly excluded:

GSM-R and Interoperability issues under the Railway Directive being handled by TC RT,
Air Traffic Management and Aeronautical issues being handled by ERM-TG25,
Maritime issues being handled by ERM-TG26,
Automotive radar issues being handled by ERM-TG31B.

Organization and Working Methods

TC ITS shall work in accordance with the normal rules as given in the ETSI Directives and, in particular, the Technical Working Procedures.
TC ITS shall prepare ETSI deliverables of the type of EG, TR, TS, ES and EN.
TC ITS shall provide progress reports to the ETSI Board and OCG from time to time.
TC ITS will liaise with other ETSI TBs (particularly with TC ERM, TC MSG, TC TISPAN, TC BRAN, and TC RT) and other SDOs, including 3GPP, ITU (APSC TELEMOV), CEN and CENELEC as appropriate.
TC ITS shall operate in accordance with the MoU with ECC. In particular, it should liaise through ERM with ECC on ITS related radio matters.

Existing related work items should remain in current Technical Bodies except where it is mutually agreed to transfer the work. Updates to existing ETSI standard deliverables should be done within the appropriate Technical Bodies and be co-ordinated with TC ITS where relevant.

Where appropriate, joint working groups with other Technical Bodies may be created to develop deliverables for submission to the lead body.

One of ‘verticals’ of Smart City.

Applies ICT to Transport sector to increase efficiency, sustainability and accessibility and raise level of safety and security.
Includes minimising environmental impact (CO2 emissions and fuel consumption) and improving traffic management.
ITS has applications in road safety, traffic control, fleet and freight management and location-based services, providing driver assistance and hazard warnings and supporting emergency services.
(In conjunction with CEN) first release of standards for initial deployment of Co-operative ITS - will enable vehicles made by different manufacturers to communicate with each other and with road infrastructure systems.

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.

1. Adoption (users base)
   Widely adopted in industry
2. Development Status
   Depends on specification, some published others under development
3. Compliance
   Having compliance testing process (include test suites, method, etc.)
4. Openness
   Open to public – most groups some only open to members

5. Ratification process (how the standard is being approved?)

Done by members and open for consultation from external parties

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
    - Organisational interoperability.

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs
    - Depends on specification

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative
    - ECC, CENELEC

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
    - Multiple domains

- Application area:
    - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
        - Different specifications cover different areas. Smart City focus in some specifications

- Scope: mapping to knowledge areas of concerns in IoT.
    - Communication and Connectivity knowledge area:
    - Integration/Interoperability knowledge area:
    - Applications knowledge area:
    - Infrastructure knowledge area:
    - IoT Architecture knowledge area:
    - Devices and sensor technology knowledge area:
    - Security and Privacy knowledge area:

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy
    - FRAND – ETSI IPR policy - http://www.etsi.org/about/how-we-work/intellectual-property-rights-iprs

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software
    - Specification open ETSI web site – free to access for all.

ETSI TC Smart M2M

- Description:
  Responsibility

  TC Smart M2M will primarily provide specifications for M2M services and applications. Much of the work will focus on aspects of the Internet of Things (IoT) and Smart Cities.
  TC Smart M2M will support European policy and regulatory requirements including mandates in the area of M2M and the Internet of Things.
  TC Smart M2M work includes 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.

  Areas of activity

  The activities of TC Smart M2M will include the following:
  Be a centre of expertise in the area of M2M and Internet of Things (IoT) to support M2M services and applications;
  Maintain ETSI M2M published specifications;
  Produce specifications as needed for regulatory purposes;
  Transpose the output of oneM2M to TC M2M.

  TC Smart M2M will aim at referring to existing work done elsewhere, or encouraging existing groups to fulfil Smart M2M requirements. The TC will undertake necessary work that is not being provided for elsewhere.

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.

  1. Adoption (users base)
     Widely adopted in industry
  2. Development Status
     Depends on specification, some published others under development
  3. Compliance
     Having compliance testing process (include test suites, method, etc.)
  4. Openness
     Open to public – most groups some only open to members

  5. Ratification process (how the standard is being approved?)
     Done by members and open for consultation from external parties

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
  - Organisational interoperability

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs
  - Depends on specification

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative

- OneM2M

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
  - Multiple domains

- Application area:
  - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
    - Different specifications cover different areas. Smart City focus in some specifications

- Scope: mapping to knowledge areas of concerns in IoT.
  - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):
    - Different specifications cover different areas:

    - Communication and Connectivity knowledge area:
    - Integration/Interoperability knowledge area:
    - Applications knowledge area:
    - Infrastructure knowledge area:
    - IoT Architecture knowledge area:
    - Devices and sensor technology knowledge area:
    - Security and Privacy knowledge area:

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy
  - FRAND – ETSI IPR policy - http://www.etsi.org/about/how-we-work/intellectual-property-rights-iprs

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software
  - Specification open ETSI web site – free to access for all.

ETSI ISG IP6 (Internet Protocol 6)

- Description:
  ETSI, the European Telecommunications Standards Institute, produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and Internet technologies.
- The ETSI ISG IP6 (Internet Protocol 6) has the ambition to define best practices, garner support and create awareness of the impact of IPv6 on critical infrastructure and on emerging topics such as Cloud Computing, IoT (Internet of Things), SDN/NFV (Software Defined Networking/Network Function Virtualization) and 5G.
- The main objectives are:

- Attract and garner support from all stakeholders worldwide to join and work on pre-standardization in a neutral membership environment with infrastructure and logistics caring also for IPR issues and working procedures
- Stimulate interoperability harmonization and coalition efforts to converge and focus the work for greater impact and exploitations for the common good
- Define best practices, focus on study and definition of requirements and use cases, garner support and create awareness of the impact of IPv6 on critical infrastructure and on emerging topics such as Cloud Computing, IoT, SDN/NFV and 5G
- Focus on IPv4-IPv6 impact in early technical discussions, integrating new technologies with a holistic approach such as IPv6-based SDN, Machine-to-Machine, Mobile Internet of Things, Mobile Cloud Computing and Fringe Internet, focusing on commonly agreed requirements toward the emergence of potential "IPv6 integration"

  For more details see: https://portal.etsi.org/tb.aspx?tbid=827&SubTB=827

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.

  1. Adoption (users base)
     No implementations
  2. Development Status
     Deliverables under development

  3. Compliance
     Not relevant, since the specifications are not normative.
  4. Openness
     Open to public

  5. Ratification process (how the standard is being approved?)
     Done by members and open for consultation from external parties

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
  - Organisational interoperability.

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs
  - It will not specify standards. It might use standards and protocols developed by other SDOs.

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative
  - Not relevant

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);

    - It can cover multiple domains

- Application area:
    - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
        - It can cover multiple domains

- Scope: mapping to knowledge areas of concerns in IoT.
    - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):
        - Communication and Connectivity knowledge area:
        - Integration/Interoperability knowledge area:
        - Infrastructure knowledge area:
        - Security and Privacy knowledge area:

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy
    - FRAND – ETSI IPR policy - http://www.etsi.org/about/how-we-work/intellectual-property-rights-iprs

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software
    - Specification open ETSI web site – free to access for all.

ETSI ISG MEC (Mobile-Edge Computing)

- Description:
  Mobile-edge Computing provides IT and cloud-computing capabilities within the RAN (Radio Access Network) in close proximity to mobile subscribers. Located at the base station or at the Radio Network Controller (RNC), it also provides access to real-time radio and network information (such as subscriber location, cell load, etc.) that can be exploited by applications and services to offer context related services; these services are capable of differentiating the mobile broadband experience. For application developers and content providers, the RAN edge offers a service environment with ultralow latency and high-bandwidth as well as direct access to real-time radio network information.

  Mobile edge computing allows content, services and applications to be accelerated, increasing responsiveness from the edge. The customer's experience can be proactively maintained through efficient network and service operations, based on insight into the radio and network conditions. Operators can open the radio network edge to third-party partners, allowing them to rapidly deploy innovative applications and services towards mobile subscribers, enterprises and other vertical segments. Proximity, context, agility and speed can be translated into value and can be exploited by mobile operators, service and content providers, Over the Top (OTT) players and Independent Software Vendors (ISVs), enabling them to play complementary and profitable roles within their respective business models and allowing them to monetize the mobile broadband experience.

This environment can create a new value chain and an energized ecosystem comprising application developers, content providers, OTT players, network equipment vendors and mobile operators. Based on innovation and business value, this value chain will allow all players to benefit from greater cooperation.

The intention is to foster dissemination of the deliverables produced by the ISG MEC in order to develop favourable market conditions which will create sustainable business for all players in the value chain, and to facilitate global market growth.

The goals of the ISG MEC are to:

- Create a standardized, open environment which will allow the efficient and seamless integration of third-party applications across multi-vendor Mobile-edge Computing platforms. This will ensure that the vast majority of the customers of a mobile operator can be served.
- Enable and accelerate the development of edge applications across the industry, increasing the market scale and improving the market economics.
- Address regulatory and legal requirements..

MEC can help accelerate and enhance smart city applications.

Example 1: Active device location tracking service:

MEC tracks active devices (independent of GPS information) and provides real-time location information & location statistics of UEs located in coverage area of MEC server,
Helps to understand how crowd is distributed,
Crowd dynamics can help with smart transportation optimization as transportation systems require (anonymous) location information from a large population. Helps with utility planning, etc.

Example 2: Intelligent video analytics at the edge:

distributed live video streams analytics at mobile edge and events are triggered automatically (e.g. movement, objects, crowd, etc.), enables fast detection and action triggering.

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.

1. Adoption (users base)
   No implementations
2. Development Status
   Specification under development
3. Compliance
   Having compliance testing process (include test suites, method, etc.)
4. Openness
   Open to public

5. Ratification process (how the standard is being approved?)
   Done by members and open for consultation from external parties

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
  - Organisational interoperability

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs
    - Depends on specification

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative
    - Not relevant

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
    - Multiple domains

- Application area:
    - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
        - Different specifications cover different areas. Smart City focus in some specifications

- Scope: mapping to knowledge areas of concerns in IoT.
    - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):

        - Infrastructure knowledge area:

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy
    - FRAND – ETSI IPR policy - http://www.etsi.org/about/how-we-work/intellectual-property-rights-iprs

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software
    - Specification open ETSI web site – free to access for all.

ETSI ISG NFV (Network Functions Virtualisation)

- Description:
  The original target of ISG NFV consisted in providing a pre-standardisation study before considering later a broader standards proposal in a new or existing standardisation group. It was important at that stage to first clearly define, agree, and share the goals of virtualising network functions with the whole industry. This was addressed in the 2013-2014 time frame, and resulted in the publication of the first ISG NFV specifications release.

  In 2015 and 2016, the purpose of ISG NFV remains to produce the technical specifications for the virtualisation of network functions.

This will be achieved by delivering both informative documents (analysis, Use Case descriptions, feasibility studies, reports, etc…) and normative documents (requirements, architecture, interface specification, etc…) aiming at helping the industry in its quest for interoperability.

Through these documents ISG NFV will address technical challenges that include:
• Ensuring that virtualised network platforms will be simpler to operate than what exists today.
• Achieving high performance virtualised network appliances which are portable between different hardware vendors, and with different hypervisors.
• Achieving co-existence with legacy hardware-based network platforms whilst enabling an efficient migration path to fully virtualised network platforms which re-use network operator BSS and OSS.
• Management and orchestration of virtual network appliances (particularly alongside legacy management systems) while ensuring security from attack and misconfiguration.
• Maintaining network stability and service levels without degradation during appliance load and relocation.
• Ensuring the appropriate level of resilience to hardware and software failures.
• Enable the creation of virtual network appliances which will run, ideally without recompilation, on any hypervisor and hardware configuration, and integrate "on the fly" into the network operators' existing EMS, NMS, OSS, BSS and orchestration systems.
ISG NFV will also perform a requirement analysis for future technical specifications & standards in ad hoc standardisation organisation & groups to be identified or created at ETSI and other relevant standards development organisations.

GS NFV 001 Use Cases identifies broad range of applications that could leverage distributed NFV Infrastructure (NFVI). Service models include multi-tenant arrangements that may provide useful paradigm for smart city services and applications to leverage. ISG NFV developing forward looking feature roadmap to understand how work can be leveraged by services and technologies developed in other industry bodies.

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.

  1. Adoption (users base)
     Reference implementations
  2. Development Status
     Specification under development
  3. Compliance
     Having compliance testing process (include test suites, method, etc.)
  4. Openness
     Open to public

  5. Ratification process (how the standard is being approved?)
     Done by members and open for consultation from external parties

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
  - Organisational interoperability.

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs
    - Depends on specification

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative
    - Not relevant

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
    - Multiple domains

- Application area:
    - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
        - Network infrastructure

- Scope: mapping to knowledge areas of concerns in IoT.
    - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):

        - Infrastructure knowledge area:

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy
    - FRAND – ETSI IPR policy - http://www.etsi.org/about/how-we-work/intellectual-property-rights-iprs

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software
    - Specification open ETSI web site – free to access for all.

ETSI ISG OEU (Operational energy Efficiency for Users)

- Description:
  The goal is to create Global Efficiency Indicators for environmentally efficient ICT, e.g. infrastructure, equipment and software within data centres and networks taking into account at least power consumption and green house gas emission.

  Energy efficiency of system installations (data centre buildings, transmission node building, computer rooms, networks and IT systems) is of high importance for the ICT Customers who are users of ICT System Installations as Car manufacturers, Banks, Insurance Companies, Network Operators, Airplane Companies, Governmental Ministries... (hereinafter the “Users”).

Independently from the ICT systems integrators, service providers, producers and manufacturers of ICT system installations, the Users, in the perspective of EU Digital Agenda mechanism and law enforcements (e.g. "carbon taxes") are proposing commonly agreed and proofed Key Performance Indicators (KPIs) and framework of implementation. For the Users, existing non-users specific indicators (Like PUE from The Green Grid association) are not comprehensive enough and not taking into account all Users' installation efforts and detailed operational constraints (external physical environment, climate and geography, redundancy, free cooling...) as well as all innovative energy efficiency techniques (e.g. increase of maximum operational temperature). With the support of ETSI ATTM members agreed in ATTM#9 Plenary meeting and the European Commission, the ETSI Members among the Users already grouped together in a non-for-profit Association (CRIP/CTO ALLIANCE) are proposing the creation of an ETSI Industry Specification Group (ISG) on "Operational energy Efficiency for Users" (OEU). This creation is done in close collaboration with other major Users like Banks, Insurance Companies..., who belong to CRIP/CTO ALLIANCE (Club des Responsables d'Infrastructures et de Production) but are not ETSI-Members

CRIP/CTO ALLIANCE is an association of ICT professionals seeking to dramatically raise the environmental efficiency of ICT areas through a series of short-term and long-term proposals. CRIP/CTO ALLIANCE proposes the use of efficiency metrics which enable ICT actors to estimate energy efficiency of their activities driving energy efficiency improvements. In collaboration with ETSI this concept is strengthened. For example, the current indicators described in ETSI TS 105 174-2-2 Clause 5.3.1 need to take into account more factors to allow useful and meaningful Key Performance Indicators (KPIs) calculation, measurement and comparisons.

Such more reliable energy efficiency KPIs will help Users of Operational Architecture to easily identify, compare and scale the effective energy efficiency of their ICT installations internally and with the other Users. Users need a better common standard KPI and way of implementation.

This ISG OEU will elaborate ETSI Group Specifications (GSs) for Energy Efficiency of Operational Architecture and framework of implementation designed, implemented and validated by Users. These Users' requirements will be provided to ETSI TCs (e.g. ATTM, EE) in order to develop ETSI standards (e.g. Global KPI definitions) for their inclusion in EU ICT Digital Agenda and proposed to all ICT communities.

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.

    1. Adoption (users base)
        Reference implementations
    2. Development Status
        Specification under development
    3. Compliance
        Having compliance testing process (include test suites, method, etc.)
    4. Openness
        Open to public

    5. Ratification process (how the standard is being approved?)
        Done by members and open for consultation from external parties

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
    - Organisational interoperability.

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs
    - Depends on specification

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative
    - Not relevant

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
    - Multiple domains

- Application area:
    - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
        - Energy efficiency

- Scope: mapping to knowledge areas of concerns in IoT.
    - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):

        - Infrastructure knowledge area:
            - Energy efficiency

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy
    - FRAND – ETSI IPR policy - http://www.etsi.org/about/how-we-work/intellectual-property-rights-iprs

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software
    - Specification open ETSI web site – free to access for all.

5.2.5 GSMA (GSM Association)

- Description: main objective and focus of initiative
  Features: high level functionalities covered by the initiative
    - http://www.gsma.com/aboutus/
    - http://www.gsma.com/connectedliving/

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai and the Mobile 360 Series conferences.
The GSMA Connected Living programme (http://www.gsma.com/connectedliving/) is an initiative to help operators add value and accelerate the delivery of new connected devices and services in the Machine to Machine (M2M) market.

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.
  1. Adoption (users base)
     - Widely adopted in industry
  2. Development Status
     - Approved with planned revisions
  3. Compliance
     - Not managed
  4. Openness
     - Open by formal membership
  5. Ratification process (how the standard is being approved?)
     - Closed process done by members only with no consultation from external parties
- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
  - Technical interoperability

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs
  - GSMA is mainly for public policy and spectrum policy lobby, mobile business development and mobile market promotion. The only one standard made by GSMA is eSIM.

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative
  - 3GPP
  - There are also more than 250 vendors and more than 800 MNOs in the GSMA. The membership types consist of Full Membership, Associate Membership and Rapporteur Membership. The full membership can be found http://www.gsma.com/membership/who-are-our-gsma-members .

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
  - GSMA make just one standard, eSIM. It locates in the connectivity domain, and can be used for both consumer and industrial market.

- Application area:
  - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
    - The GSMA is mainly for promotion of mobile industrial, which includes public policy and spectrum policy, management of mobile service, mobile API, mobile application in different vertical area of industry, and personal data.

- Scope: mapping to knowledge areas of concerns in IoT.
  - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):
    - Applications knowledge area:
    - IoT Architecture knowledge area:
    - Devices and sensor technology knowledge area:
    - Security and Privacy knowledge area:

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy

  Reference: http://www.gsma.com/newsroom/wp-content/uploads/2013/09/AA-32-v4-0.pdf

GSM Association Non-confidential
Official Document AA.32 - GSM Association Intellectual Property Rights Regulations

GSM Association Intellectual Property Rights Regulations
Version 4.0
31 August 2013

This is a Binding Permanent Reference Document of the GSMA

This is a GSMA Board owned document.

Security Classification: Non-confidential

This document is subject to copyright protection. The GSM Association ("GSMA" or "Association")) makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice. Access to and distribution of this document by the Association is made pursuant to the Regulations of the Association.

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software

  GSMA published documents available at:
  http://www.gsma.com/newsroom/gsmadocuments/

5.2.6 *HyperCat*

- Description:

HyperCat is designed for representing and exposing Internet of Things data hub catalogues over standard web technologies, to improve data discoverability and interoperability. It allows a
server to provide a set of resources identified by URIs to a client, each with a set of semantic annotations.

Technically, HyperCat is an open, lightweight JSON-based hypermedia catalogue format for exposing collections of URIs. Each HyperCat catalogue may expose any number of URIs, each with any number of RDF-like triple statements about it.

- Readiness
  - Multiple organisations/Reference Implementations

- Interoperability level
  - Semantic Interoperability

- Standards
  - The HyperCat 2.0 specification is going through the BSI PAS process (PAS 212 – Automatic resource discovery for the IoT), with a planned completion date of April 2016.

- Supporting organizations
  - A complete list of members of the HyperCat consortium is available at: http://www.hypercat.io/consortium.html. Leading members who have actively participated in specification development include: IBM, BT, Flexeye, 1248 Ltd & Thingful.

- Domain:
  - Relevant to both B2B and B2C, operates at "Service & App" level.

- Application area:
  - Integrated/complete IoT solutions (i.e. horizontal)
- Scope:
  - Integration/Interoperability knowledge area:
  - Applications knowledge area:
  - *Security and Privacy knowledge area:*

- IPR Policy Available
  - Creative Commons Attribution 4.0 International License

- Specification Access:
  - The latest publically available version can be seen at: http://www.hypercat.io/standard.html

5.2.7 IEC (International Electrotechnical Commission)

This section provides a brief description of the IEC (International Electrotechnical Commission) initiative and its IoT related Technical Committees (TCs).
IEC covers all electrotechnical aspects from plugs, wires, voltage levels to automation, control and management.

Various protocols are supported: e.g. IEC61850, IEC 61968/61970 (CIM), XMPP, DLMS/COSEM, OPC-UA, various field buses.
Various mature standards are available that are widely adopted in the industry
The important committees & groups are:

- SC3D Product properties and classes and their identification,
- TC 8 Systems aspects for electrical energy supply,
- TC13 Electrical energy measurement and control,
- TC 57 Power systems management and associated information exchange,
- TC65 Industrial-process measurement, control and automation,
- SG8 Industry 4.0 - Smart Manufacturing,
- SG 9 Communication Technologies,
- SG10 Wearable Smart Devices,
- SyC Smart Energy,
- SyC Active Assisted Living,
- SEG1 Smart Cities,
- SEG5 Electrotechnology for mobility,
- SEG6 Non-traditional Distribution Networks / Microgrids

Participation is open via the national committees.
The followed IPR regime is (FRAND).
Specifications are openly available for a fee.

IEC TC57

- Description:
  - To prepare international standards for power systems control equipment and systems including EMS (Energy Management Systems), SCADA (Supervisory Control And Data Acquisition), distribution automation, teleprotection, and associated information exchange for real-time and non-real-time information, used in the planning, operation and maintenance of power systems. Power systems management comprises control within control centres, substations and individual pieces of primary equipment including telecontrol and interfaces to equipment, systems and databases, which may be outside the scope of TC 57.
- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.
  1. Adoption (users base)
     - Widely adopted in industry
  3. Compliance
     - Not managed by IEC
  4. Openness
     - Open to public
  5. Ratification process (how the standard is being approved?)
     - Done by members and open for consultation from external parties

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
  - Syntactical interoperability
  - Technical interoperability
  - Semantic interoperability

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs .
    - Some examples:
        - IEC/TR 62357 Reference Architecture
        - IEC 61968 Application integration at electric utilities - System interfaces for distribution management
        - IEC 61970 Energy management system application program interface
        - IEC 62325 Framework for energy market communications
        - IEC61850 Communication networks and systems for power utility automation
        - IEC 62351 Power systems management and associated information exchange - Data and communications security
        - IEC 62746 Systems Interface between Customer Energy Management System and the Power Management System
- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative
    - Energy, Smart Grid, Smart Cities

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
    - Industrial
- Application area:
    - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
    - Smart Grid, Smart City

- Scope: mapping to knowledge areas of concerns in IoT.
    - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):
        - Communication and Connectivity knowledge area:
        - Integration/Interoperability knowledge area:
        - Applications knowledge area:
        - Infrastructure knowledge area:
        - IoT Architecture knowledge area:
        - Security and Privacy knowledge area:

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy
    - ITU / ISO / IEC code of practice.
    - FRAND

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software
    - Open to everyone with a fee.

IEC TC65

- Description:
  - IEC TC65, established in 1968, prepares basic standards for industrial automation as well as process
    industry specific standards. The Scopes of TC65 and its SCs are as follows:

    TC65: INDUSTRIAL PROCESS MEASUREMENT, CONTROL AND AUTOMATION

    To prepare international standards for systems and elements used for industrial process
    measurement, control and automation. To coordinate standardization activities which affect integration of components and functions into such systems including safety and security aspects. This work of standardization is to be carried out in the international fields for equipment and systems.

    SC65A: SYSTEM ASPECTS

    To prepare international standards regarding the generic aspects of systems used in industrial process measurement, control and manufacturing automation: operational conditions (including EMC), methodology for the assessment of systems, functional safety, etc.

    SC65A also has a safety pilot function to prepare standards dealing with functional safety
    of electrical/electronic/programmable electronic systems.

    SC65B: MEASUREMENT AND CONTROL DEVICES

    To prepare international standards in the field of specific aspects of devices (hardware
    and software) used in industrial process measurement and control, such as measurement devices, analysing equipment, actuators, and programmable logic controllers, and covering such aspects as interchangeability, performance evaluation, and functionality definition.

    SC65C: INDUSTRIAL NETWORKS

    To prepare international standards on wired, optical and wireless industrial networks for
    industrial-process measurement, control and manufacturing automation, as well as for instrumentation systems used for research, development and testing purposes. The scope includes cabling, interoperability, co-existence and performance evaluation.

    SC65E: DEVICES AND INTEGRATION IN ENTERPRISE SYSTEMS

    To prepare international standards specifying:

    (1) Device integration with industrial automation systems. The models developed in these standards address device properties, classification, selection, configuration,

commissioning, monitoring and basic diagnostics.

(2) Industrial automation systems integration with enterprise systems. This includes transactions between business and manufacturing activities which may be jointly developed with ISO TC184.

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.
  1. Adoption (users base)
     - Widely adopted in industry
  3. Compliance
     - Not managed by IEC
  4. Openness
     - Open to public
  5. Ratification process (how the standard is being approved?)
     - Done by members and open for consultation from external parties

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
  - Syntactical interoperability
  - Technical interoperability
  - Semantic interoperability
  - Organisational interoperability

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs

  Publication Example

  IEC 60050-351 (IEV vocabulary)
  IEC 61010 (Safety requirements for equipment)
  IEC 62443 (Cyber security)
  IEC 62708 (Documentation requirements)
  IEC 61326 (EMC)
  IEC 61508 Series (Functional Safety)
  IEC 61511 (Functional Safety process industry sector)
  IEC 61512 (Batch Control)
  IEC 61131 (PLC)
  IEC 61499 (Function Block)
  IEC 60534 (Industrial-process control valves)
  IEC 61207 (Expression of performance of gas analyzers)
  IEC 61158 Series (Fieldbus)
  IEC 61588 (Precision clock synchronization)
  IEC 61784 (Industrial communication networks – Profiles)
  IEC 61918 (Cabling)
  IEC 62439 (High availability automation networks)
  IEC 62591, IEC 62601, IEC 62734 (Wireless)
  IEC 62657 (Wireless coexistence)
  …

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative
    - Manufacturing
    - Industrial automation

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
    - Industrial

- Application area:
    - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
    - Smart manufacturing

- Scope: mapping to knowledge areas of concerns in IoT.
    - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):
        - Communication and Connectivity knowledge area*:*
        - Integration/Interoperability knowledge area:
        - Applications knowledge area:
        - Infrastructure knowledge area:
        - IoT Architecture knowledge area:
        - Devices and sensor technology knowledge area:
        - Security and Privacy knowledge area:

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy
    - ITU / ISO / IEC code of practice.
    - FRAND

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software
    - Open to everyone with a fee.

5.2.8 IEEE P2413: Standard for an Architectural Framework for the Internet of Things

- Description:
    - Defines an Architectural Framework for the IoT, including descriptions of various IoT domains, definitions of IoT domain abstractions, and identification of commonalities between different IoT domains.

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.

1. Adoption (users base)

- No implementations

2. Development Status
   - Under development
3. Compliance
   - Not managed
   - Having compliance testing process (include test suites, method, etc.)
4. Openness
   - Open by formal membership
5. Ratification process (how the standard is being approved?)
   - Done by members and open for consultation from external parties

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
  - Syntactical interoperability
  - Technical interoperability
  - Semantic interoperability
  - Organisational interoperability

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs
  - P2413 Standard for an Architectural Framework for the Internet of Things

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative
  - Not relevant
- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
  - Market: consumer and industrial,
  - Technology: closer to service & applications
- Application area:
  - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
  - Horizontal
- Scope: mapping to knowledge areas of concerns in IoT.
  - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):
    - IoT Architecture knowledge area:

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy
  - FRAND, royalty free

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software
  - Open to everyone with a fee.

5.2.9 IETF (Internet Engineering Task Force)

This section provides a brief description of the IETF (Internet Engineering Task Force) initiative and its IoT related Working Groups (WGs).
The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet. The IETF Mission Statement is documented in RFC 3935. The IETF has an IOT directorate to deal with IOT specificities.

IETF WG 6lo (IPv6 over Networks of Resource-constrained Nodes)

- Description:
  - The official website of IETF 6lo (**IPv6 over Networks of Resource-constrained Nodes (6lo)** WG can be found via: https://datatracker.ietf.org/wg/6lo/charter/.

    6lo focuses on the work that facilitates IPv6 connectivity over constrained node networks with the characteristics of:
    * limited power, memory and processing resources
    * hard upper bounds on state, code space and processing cycles
    * optimization of energy and network bandwidth usage
    * lack of some layer 2 services like complete device connectivity and broadcast/multicast

    Specifically, 6lo will work on:

    1. IPv6-over-foo adaptation layer specifications using 6LoWPAN technologies (RFC4944, RFC6282, RFC6775) for link layer technologies of interest in constrained node networks

    2. Information and data models (e.g., MIB modules) for these adaptation layers for basic monitoring and troubleshooting.

    3. Specifications, such as low-complexity header compression, that are applicable to more than one adaptation layer specification

    4. Maintenance and informational documents required for the existing IETF specifications in this space.

    Only specifications targeting constrained node networks are in scope. 6lo will work closely with the 6man working group, which will continue to work on IP-over-foo documents outside the constrained node network space and will continue to be the focal point for IPv6 maintenance. For adaptation layer specifications that do not have implications on IPv6 architecture, 6man will be notified about 6lo's working group last call. Specifications that might have such an impact (e.g., by using IPv6 addresses in a specific way or by introducing new ND options or by exposing to IPv6 a link model different from either Ethernet or 6lowpan) will be closely coordinated with 6man, and/or specific parts will be fanned out to 6man documents. Beyond 6man, 6lo will also coordinate with LWIG and INTAREA.

    6lo works on small, focused pieces of work, but does not take on larger cross-layer efforts. The working group will continue to reuse existing protocols and mechanisms whenever reasonable and possible.

    Security and management work that is not specific to the link layers being worked on is out of scope. Work related to routing is out of scope. 6lo will coordinate closely with the working groups in other areas that focus on constrained node networks, such as ROLL (RTG) and CoRE (APP).

- Readiness:

  1: Adoption (users base)
  - Reference implementations and interoperability plug test events done by ETSI

  2. Development Status
  - RFC 7557 Approved

  3. Compliance
  - Not IETF responsibility

4. Openness
    - Open to public
5. Ratification process (how the standard is being approved?)
    - Open process for all parties interested in the ratification

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
    - Syntactical interoperability
    - Technical interoperability
    - Semantic interoperability

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs

• **Date**	• **Milestone**
Apr 2015	WG adoption call for 6lo security related draft
Mar 2015	WG last call for draft-ietf-6lo-6lobac draft-ietf-6lo-6lobac
Mar 2015	WG LC for draft-ietf-6lo-dect-ule draft-ietf-6lo-dect-ule
Done	WG adoption call for draft-hong-6lo-ipv6-over-nfc draft-hong-6lo-ipv6-over-nfc
Done	WG LC for draft-ietf-6lo-btle draft-ietf-6lo-btle
Done	WG decision on adoption of draft-mariager-6lowpan-v6over-dect-ule draft-mariager-6lowpan-v6over-dect-ule
Done	WG decision on adoption for draft-schoenw-6lo-lowpan-mib draft-schoenw-6lo-lowpan-mib
Done	WG decision on adoption for draft-ietf-6man-6lobac draft-ietf-6man-6lobac
Done	WG decision on adoption for draft-brandt-6man-lowpanz draft-brandt-6man-lowpanz
Done	WG decision on adoption for draft-bormann-6lo-ghc draft-bormann-6lo-ghc

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative: 6lo is an IETF WG.

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
    - Market domain: Located on the vertical axis, to show that it is equally used by the consumer and industrial internet market.
    - Technical domain: Closer to the service&applications edge of the vertical axis

- Application area:
    - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
        - 6lo WG is focusing on horizontal industry

- Scope: mapping to knowledge areas of concerns in IoT.

- The 6lo WG can be mapped to the following knowledge areas:
  - Communication and Connectivity knowledge area:
  - Integration/Interoperability knowledge area:
  - Security and Privacy knowledge area:

- IPR Policy Available:
  - The IETF Intellectual property rules are defined in RFC 3739, "Intellectual Property Rights in IETF technology" (updated by RFC 4879)

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software :
  - Access of published (RFCs) and non-published (Internet draft) specifications for members and non-members is open and free of payment

IETF WG 6TiSCH (IPv6 over the TSCH mode of IEEE 802.15.4e)

- Description:
  - The official website of IETF 6TiSCH (**IPv6 over the TSCH mode of IEEE 802.15.4e (6tisch)**) WG can be found via: https://datatracker.ietf.org/wg/6tisch/charter/.
    Low-power and Lossy Networks (LLNs) interconnect a possibly large number of resource-constrained nodes to form a wireless mesh network. The 6LoWPAN, ROLL and CoRE IETF Working Groups have defined protocols at various layers of the protocol stack, including an IPv6 adaptation layer, a routing protocol and a web transfer protocol. This protocol stack has been used with IEEE802.15.4 low-power radios.
    The IEEE802.15.4e Timeslotted Channel Hopping (TSCH) is a recent amendment to the Medium Access Control (MAC) portion of the IEEE802.15.4 standard. TSCH is the emerging standard for industrial automation and process control LLNs, with a direct inheritance from WirelessHART and ISA100.11a. Defining IPv6 over TSCH, 6TiSCH is a key to enable the further adoption of IPv6 in industrial standards and the convergence of Operational Technology (OT) with Information Technology (IT).
    The nodes in a IEEE802.15.4e TSCH network communicate by following a Time Division Multiple Access (TDMA) schedule. A timeslot in this schedule provides a unit of bandwidth that is allocated for communication between neighbour nodes. The allocation can be programmed such that the predictable transmission pattern matches the traffic. This avoids idle listening, and extends battery lifetime for constrained nodes. Channel-hopping improves reliability in the presence of narrow-band interference and multi-path fading.
    These techniques enable a new range of use cases for LLNs, including:
    - Control loops in a wireless process control network, in which high reliability and a fully deterministic behaviour are required.
    - Service Provider networks transporting data from different independent clients, and for which an operator needs flow isolation and traffic shaping.
    - Networks comprising energy harvesting nodes, which require an extremely low and predictable average power consumption.

IEEE802.15.4e only defines the link-layer mechanisms. It does not define how the network communication schedule is built and matched to the traffic requirements of the network.
Description of Working Group:

The Working Group will focus on enabling IPv6 over the TSCH mode of the IEEE802.15.4e standard. The extent of the problem space for the WG is one or more LLNs, eventually federated through a common backbone link via one or more LLN Border Routers (LBRs). The WG will rely on, and if necessary extend, existing mechanisms for authenticating LBRs.
Initially, the WG will limit its scope to distributed routing over a static schedule. In that case, a node's schedule can be either preconfigured, or learnt by a node when joining the network, but it remains unchanged after the node has joined a network. The Routing Protocol for LLNs (RPL) is used on the resulting network.
The WG will interface with other appropriate groups in the IETF Internet, Operations and Management, Routing and Security areas.
Work Items:

The group will:
1. Produce "6TiSCH architecture" to describe the design of 6TiSCH networks. This document will highlight the different architectural blocks and signalling flows, including the operation of the network in the presence of multiple LBRs. Initially, the document will focus on distributed routing operation over a static TSCH schedule.
2. Produce an Information Model containing the management requirements of a 6TiSCH node. This includes describing how an entity can manage the TSCH schedule on a 6TiSCH node, and query timeslot information from that node. A data model mapping for an existing protocol (such as Concise Binary Object Representation (CBOR) over the Constrained Application Protocol (CoAP)) will be provided.
3. Produce "Minimal 6TiSCH Configuration" defining how to build a 6TiSCH network using the Routing Protocol for LLNs (RPL) and a static TSCH schedule. It is expected that RPL and the Objective Function 0 (OF0) will be reused as-is.
The work will include a best practice configuration for RPL and OF0 operation over the static schedule. Based on that experience the group may produce a requirements draft for OF0 extensions, to be studied in ROLL.
Non-milestone work items:

The Working Group may maintain a number of running, often-respun documents, that evolve as the technology is refined for work items that do not affect the milestone work items:
- implementers guide: this document will collect clarifying information based on input from implementers, in particular as it becomes available from interoperability events. This guide will contain information about test harnesses used for interoperability testing.
- coexistence guide: this document will provide information on how 6TiSCH can be operated in an environment shared with other protocols that use the same or a similar TSCH MAC, and/or operate on the same frequency band.

The WG will welcome requirements for dynamic timeslot operation, for example for centralized schedule computation.

- Readiness:
  1: Adoption (users base)
    - Reference implementations and interoperability plug test events done by ETSI
  2. Development Status
    - RFC 7557 Approved
  3. Compliance
    - Not IETF responsibility
  4. Openness
    - Open to public
  5. Ratification process (how the standard is being approved?)
    - Open process for all parties interested in the ratification

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
  - Syntactical interoperability
  - Technical interoperability
  - Semantic interoperability

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs

Date	Milestone
Dec 2015	6TiSCH architecture and terminology in RFC publication queue
Jun 2015	6TiSCH Minimal and 6top draft(s) in RFC publication queue
Dec 2014	Evaluate WG progress, propose new charter to the IESG
Dec 2014	Initial submission of 6TiSCH architecture to the IESG draft-ietf-6tisch-architecture
Dec 2014	Initial submission of 6TiSCH terminology to the IESG draft-ietf-6tisch-terminology
Nov 2014	Initial submission of 6TiSCH TSCH to the IESG draft-ietf-6tisch-tsch
Nov 2014	Initial submission of 6TiSCH data model for CoAP to the IESG draft-ietf-6tisch-coap
Nov 2014	Initial submission of 6top draft(s) to the IESG draft-ietf-6tisch-6top-interface
Nov 2014	Initial submission of 6TiSCH minimal configuration to the IESG draft-ietf-6tisch-minimal
Aug 2014	Submit 6TiSCH architecture for preliminary SECDIR review
Done	Submit YANG data model in 6top draft for preliminary OPSDIR review
Done	WG to adopt 6TiSCH terminology
Done	WG to adopt 6TiSCH data model for CoAP
Done	WG to adopt 6top draft(s)
Done	WG to adopt 6TiSCH minimal configuration

Date	Milestone
Done	WG to adopt 6TiSCH architecture
Done	WG to adopt IEEE802.15.4e TSCH overview

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative: 6TiSCH is an IETF WG.

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
    - Market domain: Located on the vertical axis, to show that it is equally used by the consumer and industrial internet market.
    - Technical domain: Closer to the service&applications edge of the vertical axis

- Application area:
    - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
        - 6TiSCH WG is focusing on horizontal industry

- Scope: mapping to knowledge areas of concerns in IoT.
    - The 6TiSCH WG can be mapped to the following knowledge areas:
        - Communication and Connectivity knowledge area*:*
        - Integration/Interoperability knowledge area:
        - Security and Privacy knowledge area:

- IPR Policy Available:
    - The IETF Intellectual property rules are defined in RFC 3739, "Intellectual Property Rights in IETF technology" (updated by RFC 4879)

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software :
    - Access of published (RFCs) and non-published (Internet draft) specifications for members and non-members is open and free of payment

IETF WG ACE (Authentication and Authorization for Constrained Environments)

- Description:
    - The official website of IETF ACE (Authentication and Authorization for Constrained Environments) WG can be found via: http://datatracker.ietf.org/wg/ace/charter/. The below text is copied from this charter:
      This working group aims to produce a standardized solution for authentication and authorization to enable authorized access (Get, Put, Post, Delete) to resources identified by a URI and hosted on a resource server in constrained environments. As a starting point, the working group will assume that access to resources at a resource server by a client device takes place using CoAP and is protected by DTLS. Both resource server and client may be constrained. This access will be mediated by an authorization server, which is not considered to be. Existing authentication and authorization protocols will be evaluated and used where applicable to build the constrained-environment solution.

Leveraging existing work means the working group benefits from available security analysis, implementation, and deployment experience. Moreover, a standardized solution for federated authentication and authorization will help to stimulate the deployment of constrained devices that provide increased security. This working group has the following tasks:

- Produce use cases and requirements
- Identify authentication and authorization mechanisms suitable for resource access in constrained environments.

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.
  1. Adoption (users base)
     - No implementations, yet
  2. Development Status
     - Under development
  3. Compliance
     - Having compliance testing process (include test suites, method, etc.)
     - Formal certification process
  4. Openness
     - Open to public
  5. Ratification process (how the standard is being approved?)
     - Done by members and open for consultation from external parties
     - Open process for all parties interested in the ratification

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
  - Syntactical interoperability
  - Technical interoperability

- Standards:
  - The ACE WG is specifying the Authentication and Authorization Solution" specification. Documents produced by this WG can be found via: http://datatracker.ietf.org/wg/ace/documents/
  - ACE WG Charter is approved on 16-06-2014, but no RFCs have been produced yet. This working group has the following tasks:
    - Produce use cases and requirements
    - Identify authentication and authorization mechanisms suitable for resource access in constrained environments.
  - Milestones:
    - Mar 2016 Submit "Authentication and Authorization Solution" specification to the IESG for publication as a Proposed Standard.
    - Sep 2015 (Done) submit "Use cases and Requirements" document to the IESG for publication as an Informational RFC.

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative: ACE is an IETF WG.

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis):
  - Market domain: Located on the vertical axis, to show that it is equally used by the consumer and industrial internet market.
  - Technical domain: Closer to the service&applications edge of the vertical axis

- Application area: whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2:
    - ACE WG is focusing on horizontal industry

- Scope: mapping to knowledge areas of concerns in IoT.
    - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):
        - Communication and Connectivity knowledge area:
            - Application layer, which include management associated with the connectivity area
        - Integration/Interoperability knowledge area:
            - supports common IoT features, such as publish a value or event and discover resources.
        - Security and Privacy knowledge area:
            - covers security and privacy topics

- IPR Policy Available:
    - The IETF Intellectual property rules are defined in RFC 3739, "Intellectual Property Rights in IETF technology" (updated by RFC 4879)

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software:
    - Access of published (RFCs) and non-published (Internet draft) specifications for members and non-members is open and free of payment

IETF WG CORE (Constrained RESTful Environments) WG

- Description:
    - The official website of IETF CORE (Constrained RESTful Environments) WG can be found via: http://datatracker.ietf.org/wg/core/charter/. The below text is copied from this charter: The CoRE working group will define a framework for a limited class of applications: those that deal with the manipulation of simple resources on constrained IP networks. A constrained IP network has limited packet sizes, may exhibit a high degree of packet loss, and may have a substantial number of devices that may be powered off at any point in time but periodically "wake up" for brief periods of time. As part of the framework for building these applications, the WG will define a Constrained Application Protocol (CoAP) for the manipulation of Resources on a Device. CoAP will be designed for use between Devices on the same constrained network, between Devices and general nodes on the Internet, and between Devices on different constrained networks both joined by an internet.
    - The initial work item of the WG is to define a protocol specification for CoAP that includes:
        - The ability to create, read, update and delete a Resource on a Device.
        - The ability to allow a Device to publish a value or event to another Device that has subscribed to be notified of changes, as well as the way for a Device to subscribe to receive publishes from another Device.
        - The ability to support a non-reliable multicast message to be sent to a group of Devices to manipulate a resource on all the Devices in the group.
        - The core CoAP functionality MUST operate well over UDP and UDP MUST be implemented on CoAP Devices. There may be OPTIONAL functions in CoAP (e.g. delivery of larger chunks of data) which if implemented are implemented over TCP. Applications which require the optional TCP features will limit themselves to a narrower subset of deployment cases.
        - A definition of how to use CoAP to advertise about or query for a Device's description. This description may include the device name and a list of its Resources, each with a URL, an interface description URI (pointing e.g. to a Web Application

Description Language (WADL) document) and an optional name or identifier. The name taxonomy used for this description will be consistent with other IETF work.
    - Specification for the HTTP REST based API and translation to communicate with Devices. Translation should make use of Device description information and should not need code updates to deal with new Devices.
    - Consider operational and manageability aspects of the protocol and at a minimum provide a way to tell if a Device is powered on or not.
- Readiness:
  1: Adoption (users base)
    - Reference implementations
    - Widely adopted in industry

  2. Development Status
    - Approved with planned revisions

  3. Compliance
    - Having compliance testing process (include test suites, method, etc.)
    - Formal certification process

  4. Openness
    - Open to public

  5. Ratification process (how the standard is being approved?)
    - Done by members and open for consultation from external parties
    - Open process for all parties interested in the ratification

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
  - Syntactical interoperability
  - Technical interoperability
  - Semantic interoperability

- Standards:
  The IETF CORE WG is specifying the COAP protocol. The produced documents can be retrieved via: http://datatracker.ietf.org/wg/core/documents/
  The produced IETF RFCs are:
  - RFC 6690: Constrained RESTful Environments (CoRE)
  - RFC 7252: The Constrained Application Protocol (CoAP)
  - RFC 7390: Group Communication for the Constrained Application Protocol (CoAP)

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative: CORE is an IETF WG.

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
  - Market domain: Located on the vertical axis, to show that it is equally used by the consumer and industrial internet market.
  - Technical domain: Closer to the service&applications edge of the vertical axis

- Application area:
  - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
    - CORE WG is focusing on horizontal industry

- Scope: mapping to knowledge areas of concerns in IoT.
  - The CORE WG can be mapped to the following knowledge areas:

- Communication and Connectivity knowledge area:
  - Application layer, which include management associated with the connectivity area
- Integration/Interoperability knowledge area:
  - supports common IoT features, such as publish a value or event and discover resources.
- Security and Privacy knowledge area:
  - covers security and privacy topics

- IPR Policy Available:
  - The IETF Intellectual property rules are defined in RFC 3739, "Intellectual Property Rights in IETF technology" (updated by RFC 4879)

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software :
  - Access of published (RFCs) and non-published (Internet draft) specifications for members and non-members is open and free of payment

IETF WG COSE (CBOR Encoded Message Syntax)

- Description:
  - The official website of IETF COSE (CBOR Encoded Message Syntax) WG can be found via: http://datatracker.ietf.org/wg/cose/charter/. The below text is copied from this charter.
    Concise Binary Object Representation (CBOR, RFC 7049) is a concise binary format for the serialization of data structured to an extended version of the JSON data model. COSE seeks to create CBOR-based object signing and encryption formats. One motivation for COSE was to reuse functionality from the JOSE working group using the CBOR data representation as it is more amenable to constrained nodes and constrained node networks (RFC 7228). The JOSE working group recently completed producing representations for cryptographic keys, message authentication (MACs), encryption, and digital signatures, using JSON representation. The resulting formats will not be cryptographically convertible from or to JOSE formats. This lack of a need for bit-for-bit compatibility will enable some simplification in the adaptation process. Criteria that should be considered in the decision making process, changing from JSON to CBOR encoding include:
    - Maintain the current JOSE paradigms and formatting where feasible.
    - Minimize message size, code size, and computational complexity to suit constrained environments, where this is expected to be used.
    - Improve security
    - Provide new functionality for additional use cases that were not required for JOSE.

    The WG will produce two deliverables:
    - A standards-track specification covering the same cryptographic formats from JOSE, with optimizations for constrained device processing, expressed in CBOR;
    - Registration for algorithms (such as AES-CCM-8) that are appropriate for constrained environments.

- Readiness:
  1. Adoption (users base)
     - No implementations, yet
  2. Development Status
     - Under development
  3. Compliance
     - Having compliance testing process (include test suites, method, etc.)

- Formal certification process

4. Openness
   - Open to public
5. Ratification process (how the standard is being approved?)
   - Done by members and open for consultation from external parties
   - Open process for all parties interested in the ratification

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
  - Syntactical interoperability
  - Technical interoperability

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs
  - The IETF COSE WG is working on a standards-track specification covering the same cryptographic formats from JOSE, with optimizations for constrained device processing, expressed in CBOR. Documents produced by this WG can be found via: http://datatracker.ietf.org/wg/cose/documents/
  - The COSE WG charter has been approved on 3rd of June 2015, but no RFCs have been produced yet. This working group has the following tasks on producing:
    - A standards-track specification covering the same cryptographic formats from JOSE, with optimizations for constrained device processing, expressed in CBOR;
    - Registration for algorithms (such as AES-CCM-8) that are appropriate for constrained environments.
  - Milestones:
    - Jan 2016 Submit COSE constrained-appropriate algorithms to the IESG, for publication as a Proposed Standard
    - Jan 2016 Submit COSE specification to the IESG, for publication as a Proposed Standard
    - Jun 2015 Submit COSE constrained-appropriate algorithms as a WG item
    - Jun 2015 Submit COSE specification as a WG item

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative: COSE is an IETF WG.

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
  - Market domain: Located on the vertical axis, to show that it is equally used by the consumer and industrial internet market.
  - Technical domain: Closer to the service&applications edge of the vertical axis

- Application area: whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2:
  - COSE WG is focusing on horizontal industry

- Scope: mapping to knowledge areas of concerns in IoT.
  - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):
    - Communication and Connectivity knowledge area:
      - Application layer, which include management associated with the connectivity area

- Integration/Interoperability knowledge area:
  - supports common IoT features, such as publish a value or event and discover resources.
- Security and Privacy knowledge area:
  - covers security and privacy topics

- IPR Policy Available:
  - The IETF Intellectual property rules are defined in RFC 3739, "Intellectual Property Rights in IETF technology" (updated by RFC 4879)

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software:
  - Access of published (RFCs) and non-published (Internet draft) specifications for members and non-members is open and free of payment

IETF WG Deterministic Networking (DetNet))

- Description:

The official website of IETF DetNet (**Deterministic Networking (DetNet))** WG can be found via: https://datatracker.ietf.org/wg/DetNet/charter/.

The Deterministic Networking (DetNet) Working Group focuses on deterministic data paths that operate over Layer 2 bridged and Layer 3 routed segments, where such paths can provide bounds on latency, loss, and packet delay variation (jitter), and high reliability. The Working Group addresses Layer 3 aspects in support of applications requiring deterministic networking. The Working Group collaborates with IEEE802.1 Time Sensitive Networking (TSN), which is responsible for Layer 2 operations, to define a common architecture for both Layer 2 and Layer 3. Example applications for deterministic networks include professional and home audio/video, multimedia in transportation, engine control systems, and other general industrial and vehicular applications being consider by the IEEE 802.1 TSN Task Group.

The Working Group will initially focus on solutions for networks that are under a single administrative control or within a closed group of administrative control; these include not only campus-wide networks but also can include private WANs. The DetNet WG will not spend energy on solutions for large groups of domains such as the Internet.

The Working Group will specify an overall architecture that encompasses the data plane, OAM (Operations, Administration, and Maintenance), time synchronization, management, control, and security aspects which are required to enable a multi-hop path, and forwarding along the path, with the deterministic properties of controlled latency, low packet loss, low packet delay variation, and high reliability. The work applies to point-to-point (unicast) and point-to-multipoint (multicast) flows which can be characterized in a manner that allows the network to 1) reserve the appropriate resources for the flows in advance, and 2) release/reuse the resources when they are no longer required. The work covers the characterization of flows, the encapsulation of frames, the required forwarding behaviours, as well as the state that may need to be established in intermediate nodes. Candidate Layer 3 data plane

technologies that may be used, without modification, include: IP and MPLS.

The working group will document which deployment environments and types of topologies are within (or outside) the scope of the DetNet architecture. This work focuses on the data plane aspects and is independent from any path setup protocol or mechanism. The data plane will be compatible with the work done in IEEE802.1 TSN.

The Working Group's scope explicitly excludes modifications of transport protocols, OAM, Layer 3 forwarding, encapsulations, and control plane protocols.

DetNet is chartered to work in the following areas:

Overall architecture: This work encompasses the data plane, OAM, time synchronization, management, control, and security aspects.

Data plane: This work will document how to use IP and/or MPLS to support a data plane method of flow identification and packet forwarding over Layer 3.

Data flow information model: This work will identify the information needed for flow establishment and control and be used by a reservation protocol or by YANG data models. The work will be independent from the protocol(s) used to control the flows (e.g. YANG+NETCONF/RESTCONF, PCEP or GMPLS).

Identification of additional YANG models: This work will document device and link capabilities (feature support) and resources (e.g. buffers, bandwidth) for use in device configuration and status reporting. Such information may also be used when advertising the deterministic network elements to a control plane. Control plane related information will be independent from the protocol(s) which may be used to advertise this information (e.g. IS-IS or GMPLS extensions). Any new YANG models will be coordinated with the Working Groups that define any augmented base models.

As needed, problem statement: This effort will establish the deployment environment and deterministic network requirements.

As needed, vertical requirements: This effort will detail the requirements for deterministic networks in various industries, for example, professional audio, electrical utilities, building automation systems, wireless for industrial applications.

To investigate whether existing data plane encryption mechanisms can be applied, possibly opportunistically, to improve security and privacy.

The WG coordinates with other relevant IETF Working Groups, including CCAMP, PCE, PALS, TEAS, OSPF, IS-IS, TSVWG, and 6TisSCH. As the work progresses, requirements may be provided to the responsible Working Group, e.g. PCE, TEAS, and CCAMP, with DetNet acting as a focal point to maintain the consistency of the overall architecture. The WG will liaise with appropriate groups in IEEE and other Standards Development Organizations (SDOs).

WG deliverables include:

As standard track or informational RFCs

Overall architecture
Data plane specification
Data flow information model
YANG model augmentations

WG sustaining/informational documents may include:

These documents may not necessarily be published, but may be maintained in a draft form or on a collaborative Working Group wiki to support the efforts of the Working Group and help new comers:

Problem statement and (constrained) deployment environments
User-driven use cases

- Readiness:
  1: Adoption (users base)
    - Working Group not officially formed
  2. Development Status

draft-finn-detnet-problem-statement-03
Deterministic Networking Problem Statement

draft-gunther-detnet-proaudio-req-01
Deterministic Networking Professional Audio Requirements

draft-korhonen-detnet-telreq-00
Deterministic networking for radio access networks

draft-wetterwald-detnet-utilities-reqs-02
Deterministic Networking Uitilities requirements

draft-zha-detnet-use-case-00
Deterministic Networking Use Case in Mobile Network

draft-dujovne-detnet-gap-analysis-01

- 3. Compliance
    - Not IETF responsibility

  4. Openness
    - Open to public

  5. Ratification process (how the standard is being approved?)
    - Open process for all parties interested in the ratification

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
    - Syntactical interoperability
    - Technical interoperability
    - Semantic interoperability

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative: DetNet is an IETF WG.

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
    - Market domain: Located on the vertical axis, to show that it is equally used by the consumer and industrial internet market.
    - Technical domain: Closer to the service&applications edge of the vertical axis

- Application area:
    - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
        - DetNet WG is focusing on horizontal industry

- Scope: mapping to knowledge areas of concerns in IoT.
    - The DetNet WG can be mapped to the following knowledge areas:
        - Communication and Connectivity knowledge area:
            - Application layer, which include management associated with the connectivity area
        - Integration/Interoperability knowledge area:
            - supports common IoT features, such as publish a value or event and discover resources.
        - Security and Privacy knowledge area:
            - covers security and privacy topics

- IPR Policy Available:
  - The IETF Intellectual property rules are defined in RFC 3739, "Intellectual Property Rights in IETF technology" (updated by RFC 4879)

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software :
  - Access of published (RFCs) and non-published (Internet draft) specifications for members and non-members is open and free of payment

IETF WG Dice (DTLS In Constrained Environments)

- Description:
  The official website of IETF Dice (**DTLS In Constrained Environments (Dice))** WG can be found via: https://datatracker.ietf.org/wg/dice/charter/.

  The Constrained Application Protocol (CoAP) can be used to manipulate resources on a device in constrained environments secured by Datagram Transport Layer Security (DTLS, RFC 6347). The DTLS In Constrained Environments (DICE) working group focuses on supporting the use of DTLS Transport-Layer Security in these environments. Constrained environments looked at in DICE include constrained devices (e.g. memory, algorithm choices) and constrained networks (e.g. PDU sizes, packet loss).

  The first task of the working group is to define a DTLS profile that is suitable for Internet of Things applications and is reasonably implementable on many constrained devices.

  The second task of the working group is to define how DTLS record layer can be used to transmit multicast messages securely. Security for these multicast messages is needed in many Internet of Things environments, as some messages are commonly multicast among a set of receivers. Session keys are needed in order to use the DTLS record layer in this way. Changes to the DTLS handshake to support this may be needed in future but are not part of the initial charter for DICE WG.

  The third task of the working group is to investigate practical issues around the DTLS handshake in constrained environments. Many current systems end up fragmenting messages, and the re-transmission and re-ordering of handshake messages results in significant complexity and reliability problems. Additional reliability mechanisms for transporting DTLS handshake messages are required as they will ensure that handling of re-ordered messages needs to be done only once in a single place in the stack. The DICE working group may also look at alternative TLS transports in cooperation with the TLS WG.

  The DTLS state machine should not be modified and key management (including for multicast security) and multi-cast session setup are out the scope for the initial work.

  The DICE working group will work closely with the TLS, CoRE and LWIG working groups.

- Readiness:
  1: Adoption (users base)
  - Widely used in the industry

2. Development Status
   draft-ietf-dice-profile-16
- 3. Compliance
  - Not IETF responsibility
4. Openness
  - Open to public
5. Ratification process (how the standard is being approved?)
  - Open process for all parties interested in the ratification

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
  - Syntactical interoperability
  - Technical interoperability
  - Semantic interoperability

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs

Date	Milestone
Jun 2014	Secure group communication specification submitted to the IESG for publication as standards track
May 2014	DTLS for IoT profile specification submitted to the IESG for publication as standards track
Dec 2013	WG document for secure group communication for IoT
Dec 2013	WG document for DTLS for Constrained Environments profile

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative: Dice is an IETF WG.

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
  - Market domain: Located on the vertical axis, to show that it is equally used by the consumer and industrial internet market.
  - Technical domain: Closer to the service&applications edge of the vertical axis

- Application area:
  - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
    - Dice WG is focusing on horizontal industry

- Scope: mapping to knowledge areas of concerns in IoT.
  - The Dice WG can be mapped to the following knowledge areas:

- Communication and Connectivity knowledge area:
  - Application layer, which include management associated with the connectivity area
- Integration/Interoperability knowledge area:
  - supports common IoT features, such as publish a value or event and discover resources.
- Security and Privacy knowledge area:
  - covers security and privacy topics

- IPR Policy Available:
  - The IETF Intellectual property rules are defined in RFC 3739, "Intellectual Property Rights in IETF technology" (updated by RFC 4879)

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software :
  - Access of published (RFCs) and non-published (Internet draft) specifications for members and non-members is open and free of payment

5.2.10 IRTF (Internet Research Task Force): T2T RG (Thing to Thing) proposed RG

- Description:
  - The T2T (Thing to Thing) proposed RG is not yet an official IRTF Research Group, but it can become an official one if there is satisfactory participation. More details regarding the T2T RG can be found via: https://github.com/t2trg/2015-ietf92
    The T2t RG will investigate open research issues in turning a true "Internet of Things" into reality, and on an Internet where low-resource nodes ("Things", "Constrained Nodes") can communicate among themselves and with the wider Internet, in order to partake in permissionless innovation.
    The focus of this RG will be on issues that touch opportunities for standardization in the IETF
    - start at the adaptation layer connecting devices to IP, and
    - end at the application layer with architectures and APIs for communicating and making data and management functions (including security functions) available.

    The main areas of interest are:
    - Understanding and managing the motivation for single purpose silos and gateways; facilitating a move towards small pieces loosely joined (hence "thing-to-thing"); scaling the number of applications in a single network
    - Deployment considerations; scaling considerations; cost of ownership
    - Management and Operation of Things
    - Lifecycle aspects (including, but not limited to, security considerations)
    - Cooperation with W3C, e.g. on data formats and semantics

- Readiness:
  1. Adoption (users base)
     - No implementations, yet
  2. Development Status
     - Under development

3. Compliance
    - Having compliance testing process (include test suites, method, etc.)
    - Formal certification process
4. Openness
    - Open to public
5. Ratification process (how the standard is being approved?)
    - Done by members and open for consultation from external parties
    - Open process for all parties interested in the ratification

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
    - Syntactical interoperability
    - Technical interoperability
    - Semantic interoperability

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs
    - The T2T RG is a proposed IRTF Research Group that will be using and providing input mainly to IETF, but also to the IOT research community. It has not produced any RFCs yet.

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative: T2T (proposed) RG is belonging to IRTF that is closely cooperating with the IETF and it represents the research activities of IETF.

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
    - Market domain: Located on the vertical axis, to show that it is equally used by the consumer and industrial internet market.
    - Technical domain: Closer to the service&applications edge of the vertical axis

- Application area: whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
    - IRTF T2T RG is focusing on horizontal industry

- Scope: mapping to knowledge areas of concerns in IoT.
    - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):
        - Communication and Connectivity knowledge area:
            - Application layer, which include management associated with the connectivity area
        - Integration/Interoperability knowledge area:
            - supports common IoT features, such as publish a value or event and discover resources.
        - IoT Architecture knowledge area:

    - plans to cover integrated/complete IoT specification solutions, including architecture descriptions. However, this is not yet agreed.
  - Security and Privacy knowledge area:
    - covers security and privacy topics

- IPR Policy Available:
  - The IRTF follows the IETF Intellectual Property Rights (IPR) disclosure rules, https://irtf.org/ipr. This is a summary of these rules as they relate to IRTF research group discussions, mailing lists and Internet Drafts:
    - If you include your own or your employer's IPR in a contribution to an IRTF research group, then you must file an IPR disclosure with the IETF.
    - If you recognize your own or your employer's IPR in someone else's contribution and you are participating in the discussions in the research group relating to that contribution, then you must file an IPR disclosure with the IETF. Even if you are not participating in the discussion, the IRTF still requests that you file an IPR disclosure with the IETF.
    - Finally, the IRTF requests that you file an IPR disclosure with the IETF if you recognize IPR owned by others in any IRTF contribution.
  - The IRTF expects that you file IPR disclosures in a timely manner, i.e., in a period measured in days or weeks, not months. The IRTF prefers that the most liberal licensing terms possible are available for IRTF Stream documents, see RFC 5743. You may file an IPR disclosure here: http://www.ietf.org/ipr/file-disclosure

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software
  - Access of published (RFCs) and non-published (Internet draft) specifications for members and non-members is open and free of payment

5.2.11 International Telecommunication Union – Telecommunication Standardization Sector (ITU-T)

- Description: International Telecommunication Union – Telecommunication Standardization Sector (ITU-T)
  The Study Groups of ITU-T assemble experts from around the world to develop international standards known as ITU-T Recommendations which act as defining elements in the global ICTs.
  ITU-T Study Group 20 ["IoT and its applications including smart cities and communities (SC&C)"], established in June 2015 and holding its first meeting in October 2015, is going to become the central venue of IoT standardization activities within ITU-T.
  SG20 will work to address the standardization requirements of Internet of Things (IoT) technologies, with an initial focus on IoT applications in smart cities and communities (SC&C).
  SG20, via the Joint Coordination Activity on Internet of Things whose supervision has been assigned to SG20, will ensure the coordination of IoT related studies across the various involved ITU-T Study Groups as well as with external SDOs, Alliances and Consortia.
  Specific study items of SG20 will include:
  - the development of international standards to enable the coordinated development of IoT technologies, including machine-to-machine communications and ubiquitous sensor networks. A central part of this study is the standardization of end-to-end

architectures for IoT, and mechanisms for the interoperability of IoT applications and datasets employed by various vertically oriented industry sectors.
- the development of standards that leverage IoT technologies to address urban-development challenges.

The IoT related specifications already published by ITU-T and the main IoT related activities of ITU-T have essentially involved Study Group 11, Study Group 13, Study Group 16 and Study Group 17 (the key involved Study Groups - September 2015 status):
- SG11 has focused on the interoperability, protocol and testing aspects of IoT;
- SG13 has mainly focused on the network aspects of IoT;
- SG16 has mainly focused on the application aspects of IoT;
- SG17 has focused on the security aspects of IoT.

Other IoT related activities have been progressed within specific ITU-T Focus Groups which, by nature, do not generate standards: the main IoT related Focus Groups (now closed) have been the Focus Group on M2M Service Layer, the Focus Group on Smart Water Management and the Focus Group on Smart Sustainable Cities.
Other complementary IoT activities have been progressed within Study Group 15 (Smart Grid and Home Network aspects) and the Collaboration on ITS Communication Standards.
Future IoT activities are expected to involve also Study Group 2 (naming, numbering, addressing and identification; service definitions) and Study Group 3 (tariff and economic aspects).

- Readiness: *(for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.*
  1. Adoption (users base)
     - No implementations/Reference implementations/Widely adopted in industry (according to the particular specification)
  2. Development Status
     - Under development/ Approved with no planned revisions/ Approved with planned revisions (according to the particular specification)
  3. Compliance
     - Not managed/Having compliance testing process (according to the particular specification). No process implemented yet for any IoT related specification.
  4. Openness
     - Open by formal membership
  5. Ratification process (how the standard is being approved?)
     - Closed process done by members only with no consultation from external parties

     NOTE – In some specific cases, it can be done by members and open for consultation from external parties, previous agreement with the external parties.

- Interoperability level: *identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:*
  - Technical interoperability/Syntactical interoperability (according to the particular specification)

  NOTE – Some specific ongoing studies are considering Semantic interoperability aspects (to be completed).

- Standards: *standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols,*

or whether they are using and integrating standards and protocols developed by other SDOs

Various standards have been proposed in published specifications (and others are considered in some ongoing studies). to be completed

Some published specifications use and integrate standards and protocols developed by other SDOs (and other SDOs' standards and protocols are considered in some ongoing studies). to be completed

List of main published specifications to be added

- Supporting organizations *(mainly for Alliances/OSS): main organizations that back the initiative*
    - Telecommunication Hardware and Software Providers
    - Service Providers, Network Providers, *Application Provider, Integrators*
    - Member State entities (Administration entities, Academies, Public Research)
    - National Regulation Authorities
    - Other National and Regional Entities
- Domain: *position the initiative, with respect to the four quadrants, see Figure 1 in Section 0, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);*
    - Most of the activities target the market without specific focus on consumer versus industrial internet - some special cases to be provided.
    - Both sides of the technology domain are targeted, according to the particular specification.

- Application area: *whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2*
    - Focus on integrated/complete IoT solutions, i.e. horizontal industry: numerous activities (in all involved Study Groups, including SG20);
    - Focus on particular vertical industries (September 2015status): Home/Building (SG13, SG15), Vehicular/Transportation (SG16), Healthcare (SG13, SG16), Cities (SG20), Farming/Agrifood (SG13). NOTE – In perspective, SG20 will be involved in all vertical industries.

- Scope: *mapping to knowledge areas of concerns in IoT. The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):*
    - All knowledge areas are concerned. At present time, the involved key Study Groups have mainly focused their activities, respectively, in the following areas:
        - *Communication and Connectivity knowledge area:* SG11, SG13, (SG20)
        - *Integration/Interoperability knowledge area:* SG11, SG13, (SG20)
        - *Applications knowledge area:* SG13, SG16, (SG20)
        - *Infrastructure knowledge area:*SG11, SG13, (SG20)
        - *IoT Architecture knowledge area:* SG11, SG13, SG16, (SG20)
        - ***Devices and sensor technology knowledge area:* SG16**
        - *Security and Privacy knowledge area:* SG17, (SG20)

- IPR Policy Available: *mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy*
    - ITU / ISO / IEC code of practice.

- Specification Access: *Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software*
  - Published specifications: the vast majority is accessible to all free of charge once a final editing process is complete. Texts that are not free of charge include common ITU-T | ISO / IEC texts for which special arrangements exist.
  - Non-published specifications: freely accessible to members only; not accessible to non-members.

5.2.12 (ISO/IEC) JTC1/WG10 Internet of Things

- Description:
  - ISO and IEC have a joint technical committee called JTC 1. JTC1 is a member based organization with the possibility of one member from each country. In 2015 JTC1 had 76 members. Standardization in JTC1 is builds on the WTO agreements on Technical Barriers to Trade.
  - In 2012 ISO/IEC JTC 1 initiated preparatory work in the field of IoT. At the JTC1 meeting in November 2014 the IoT report was accepted as presented by all members of JTC1. As a consequence of the report and its acceptance, JTC1 decided to establish a working group on IoT with the mandate to develop foundational standards.

- Mission Statement:
  - The working group has prepared a Strategic business plan but it will be confirmed at the upcoming JTC1 meeting in October in China. Until then the WG has the mandate to develop one standard which has got the following title and scope:
    Title: Information technology – Internet of Things Reference Architecture (IoT RA)
    Scope of the proposed deliverable – This new work item specifies IoT Conceptual Model, conceptual reference model, and reference architecture from different architectural views, common entities, and interfaces between IoT domains

- Business Impact:
  - All business will benefit from an international IoT standard provided from an conceptual to business specific IoT Architectures

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.
  1. Adoption (users base)
     - Developing use cases as considerations for Reference Architecture
     - The ISO/IEC JTC 1 standard is expected to be widely adopted in industry

  2. Development Status
     - In progress

  3. Compliance
     - Through 13external and 11internal liaisons with other SDO's receiving input that balance with own work for selecting solutions to standards issues
  4. Openness
     - Every standard document passes 6 stages to be realized as an international standard. National experts comment the documents at every stage for quality

completeness etc. National bodies vote on the document on every stage to insure quality and acceptance.
- Approved standards document are available through subscription or purchase

5. Ratification process (how the standard is being approved?)
   - Every formal step in developing of the standard is done by national experts.
   - The documents are casted and formally voted and commented on by national bodies. Comments and votes are being handled according to ISO/IEC Directives by the national body in charge of the secretariat.

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative
  - Syntactical interoperability
  - Technical interoperability

- Standards: will include functions for technical as well as Syntactical interoperability.
  - It is also possibly that the standard will have opening for both semantic and pragmatic interoperability levels.

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative:

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
  - Market domain: ISO/IEC JTC 1 standards document will benefit horizontal axis
  - Technical domain: ISO/IEC JTC 1 standards document will benefit all IoT – systems and integration on several interoperability levels

- Application area: whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
  - The ISO/IEC JTC 1 standards document will benefit horizontal industries

- Scope: mapping to knowledge areas of concerns in IoT.
  - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):
    - Communication and Connectivity knowledge area:
      - Good knowledge in the Communication and Connectivity
    - Infrastructure knowledge area:
      - Good knowledge in Infrastructure area

- IPR Policy Available:
  http://www.iso.org/iso/home/standards_development/resources-for-technical-work.htm
  https://connect.iso.org/display/ipr/Intellectual+Property

- Specification Access: JTC1 standards are publicly available for everyone. They can be bought thru the National Standardization Bodies or thru ISO.

- Members of a National Standardization Body who is mirroring the WG10 work will have full access to all working documents and drafts in the development process thru a web platform. Please note that liaisons to WG10 will have access to the same web platform as WG10 experts.
- Non members: cannot get access to draft standards or other working documents but can get access to all published standards.

5.2.13 OIC (Open Interconnect Consortium)

- Description:
  The open interconnect consortium founded by leading technology companies with the goal of defining the connectivity requirements and ensuring interoperability of the billions of devices that will make up the emerging internet of things (IOT).

  The Open Interconnect Consortium define and promote a single connectivity framework to enable communications and interoperability in support of the "Internet of Things" across multiple vertical markets, operating systems, platforms, modes of communication, transports and use cases and to encourage the development and distribution of products implementing such connectivity frameworks.

  The above goal will be accomplished through the following activities and outputs:

  - Specifications. Development and publication of Specifications (as defined more fully in the Intellectual Property Rights Policy of the Corporation), which define and promote communication and interoperability requirements for the "Internet of Things."
  - Open Source Project. Cooperate with open source projects in the development of open source software in support of the Specifications.
  - Test Tools: Technical resources, such as software in binary and/or source code form, for validating compliance with Specifications and open source projects.
  - Testing Activities: "Plugfests" and other events and activities that provide opportunities for Members to test interoperability and validate compliance with Specifications and open source projects.
  - Whitepapers: Technical and non-technical documents which discuss various technical and business considerations, insights, and consumer requirements for the "Internet of Things."
  - Ecosystem Development: Representing the Corporation and activities to attract industry membership and broad adoption.
  - Marketing and Public Relations: Representing the Corporation, generating awareness of the Corporation, and providing liaison to other standards development organizations.
  - Certification and Logo Program: Following publication of Specifications and open source projects, the Corporation will further develop a formal certification process, logo, trademark, and other marketing programs and collateral, the extent of which shall be determined by the Corporation, for promotion of Member products that comply with Specifications and open source projects.

  The following sets forth the technical scope of the specifications:

  Enabling devices, services and applications ("Products") to discover, connect, communicate and interoperate through:
  A framework that includes:

- Object models for devices, users, resources
- Discovery of and interaction between objects
- Associated security (authentication; encryption; privacy; access control)
- Device management (provisioning)
- Data management
- Mapping of the above onto multiple underlying technologies, but not the definition of those technologies (Bluetooth, Wi-Fi, IP, Zigbee, ZWave, etc…)
- Protocols, data formats and the mapping and adapting of both
- APIs
- Functions, input parameters, data structures, and services (including web services, web resources and software modules), to the extent that they are specifically described in detail

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.

  1. Adoption (users base)
     - Reference implementations
  2. Development Status
     - Approved with planned revisions
  3. Compliance
     - Formal certification process
  4. Openness
     - Open by formal membership
  5. Ratification process (how the standard is being approved?)
     - Closed process done by members only with no consultation from external parties

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
  - Organisational interoperability. Note work is ongoing to interoperate through the OneM2M platform as well as across the OIC ecosystem

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs

  - Combination of existing IETF and W3C standards with additional work

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative
  - Working with OneM2M

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
  - Multiple domains – initial release has a consumer focus with a mix of connectivity and services.

- Application area:
  - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
    - Different specifications cover different areas. The initial focus is on Smart Home

- Scope: mapping to knowledge areas of concerns in IoT.
  - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):
    - Communication and Connectivity knowledge area:
    - Integration/Interoperability knowledge area:
    - Applications knowledge area:
    - Infrastructure knowledge area:
    - IoT Architecture knowledge area:
    - Devices and sensor technology knowledge area:
    - Security and Privacy knowledge area:

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy
  - FRAND – Free licensing

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software
  - Specification open on OIC web site – free to access for all.

5.2.14 OneM2M

- Description: main objective and focus of initiative
  - Following text from: http://www.onem2m.org/about-onem2m/why-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. A critical objective of oneM2M is to attract and actively involve organizations from M2M-related business domains such as: telematics and intelligent transportation, healthcare, utilities, industrial automation, smart homes, etc. Initially, oneM2M shall prepare, approve and maintain the necessary set of Technical Specifications and Technical Reports for:
    - Use cases and requirements for a common set of Service Layer capabilities;
    - Service Layer aspects with high level and detailed service architecture, in light of an access independent view of end-to-end services;
    - Protocols/APIs/standard objects based on this architecture (open interfaces & protocols);
    - Security and privacy aspects (authentication, encryption, integrity verification);

- Reachability and discovery of applications;
- Interoperability, including test and conformance specifications;
- Collection of data for charging records (to be used for billing and statistical purposes);
- Identification and naming of devices and applications;
- Information models and data management (including store and subscribe/notify functionality);
- Management aspects (including remote management of entities); and
- Common use cases, terminal/module aspects, including Service Layer interfaces/APIs between:
    - Application and Service Layers;
    - Service Layer and communication functions

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.
    1. Adoption (users base)
        - Reference implementations
        - Widely adopted in industry
    2. Development Status
        - Approved with planned revisions
    3. Compliance
        - Having compliance testing process (include test suites, method, etc.)
            - oneM2M has developed a set of specifications for interoperability test, and the corresponding test event has been organized.
            - oneM2M is currently working on the compliance test specification development and held already an interop event that attracted participation of 30 companies
        - Formal certification process
            - under investigation/discussion by oneM2M
    4. Openness
        - Open to public
    5. Ratification process (how the standard is being approved?)
        - Done by members and open for consultation from external parties

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
    - Syntactical interoperability
    - Technical interoperability
    - Semantic interoperability

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs
    - oneM2M R1 supports HTTP, CoAP and MQTT as the transport protocol bindings for native oneM2M interfaces over oneM2M Mca and Mcc reference points.
    - oneM2M also adopts OMA DM (1.x/ 2.0), OMA LWM2M, BBF TR-069 as the alternative device management protocols in the case of reusing underlying network services over oneM2M Mcn reference point.

- The latest work in oneM2M includes WebSocket protocol binding over Mca and Mcc, and specifies the use if W3C semantic web technologies (e.g. RDF/OWL/SPARQL) for IoT semantic interoperability: semantic annotation, semantic discovery, ontologies, etc.

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative
  - Partner Type 1:
    - Alliance for Telecommunications Industry Solutions (ATIS)
    - Association of Radio Industries and Businesses (ARIB)
    - China Communications Standards Association (CCSA)
    - European Telecommunications Standards Institute (ETSI)
    - Telecommunications Industry Association (TIA)
    - Telecommunications Standards Development Society (TSDSI)
    - Telecommunications Technology Association (TTA)
    - Telecommunications Technology Committee (TTC)
  - Partner Type 2:
    - Broadband Forum
    - Continua
    - GlobalPlatform
    - Home Gateway Initiative (HGI)
    - New generation M2M consortium
    - Open Mobile Alliance (OMA)
  - Associate Members:
    - Ministry of Science, ICT and Future Planning (MSIP)
    - National Institute of Standards and Technology (NIST)
    - State Secretariat of Telecommunications and for the Information Society, Spain
    - United States Department of Transportation
  - There are also more than 200 member companies/institutes supporting this work. See the full member list at: http://www.onem2m.org/membership/current-members

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
  - oneM2M is positioned at the horizontal service domain (layer), which provides common service functionalities for IoT applications across vertical market domains.
  - As providing horizontal service layer technologies, oneM2M aims to cover a wide market range across both consumer and industrial domains.

- Application area:
  - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
    - oneM2M is not chartered to focus on a particular vertical industry. It shall provide standardized common service layer technologies that are applicable to various industry domains including the cross domain interactions, i.e. horizontal industry.

- However, it also investigates some selected vertical industries (e.g. home, industrial, and vehicle) in deep to ensure the provided standard/technology can fulfil the vertical requirements and interwork with the applications/network/devices in those industries. More industries may be investigated in the future.

- Scope: mapping to knowledge areas of concerns in IoT.
  - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):
    - Integration/Interoperability knowledge area:
    - Applications knowledge area:
    - IoT Architecture knowledge area:
    - Devices and sensor technology knowledge area:
    - Security and Privacy knowledge area:

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy
  - Reference: http://www.onem2m.org/images/files/oneM2M_Partnership_Agreement.pdf

2 General Principles

All the Partners have the objective, within oneM2M, to create Technical Specifications and Technical Reports that are based on solutions which best meet the technical objectives of oneM2M. All the Partners Type 1 of oneM2M have IPR policies that support a FRAND IPR regime. The IPR policies of each of the Partners Type 1 of one M2M also recognize the importance of respecting the rights of owners of essential/potentially essential IPRs. Thus, the IPR policies seek to balance such rights with the ability of implementers to access essential IPRs under Fair, Reasonable and Non-Discriminatory (FRAND) terms and conditions.

Consistent with the foregoing general principles, the following shall apply to the operations of oneM2M.

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software
  - oneM2M published documents available at: http://www.onem2m.org/technical/published-documents
  - oneM2M latest drafts available at: http://www.onem2m.org/technical/latest-drafts

5.2.15 OSGi Alliance

- Description: main objective and focus of initiative
  - not for profit SDO. The OSGi Alliance is a worldwide consortium advancing a proven and mature process to create open specifications. These specifications enable dynamic end-to-end connectivity and facilitate the componentization of software and applications, thus increasing development productivity, reducing time to market and substantially decreasing the long term maintainability costs of the resulting modular solution. The technology also provides flexible remote management and interoperability for applications and services over a broad variety of devices. Member company industries include leading service and content providers, infrastructure/network operators, utilities, enterprise software vendors, software developers, gateway suppliers, consumer electronics/device suppliers (wired and wireless) and research institutions.

Features: high level functionalities covered by the initiative

- OSGi inherently responds to many requirements of the IoT. Its most important features can be listed as:
  - A Modular execution environment enabling functional reuse of components across diverse platforms
  - A flexible Capabilities / Requirements model that enables environment-aware deployment and dependency management.
  - A dynamic environment allowing system components to be updated and/or reconfigured without restarting them
  - Lifecycle aware components that are able to respond to changes in their environment, for example the addition/activation of a hardware device
  - Support for dynamic deployment of native libraries based on the discovered system capabilities.
  - A defined security model for determining whether software modules are trusted and the actions they are permitted to perform
  - Common API's for device connectivity using various underlying communication protocols
  - A standardised common remote management interface using a variety of protocols including JMX and HTTP/REST
  - Programming models for distributed environments using synchronous or asynchronous invocations. Suitable for use in edge or cloud environments.

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2)
  - Adoption: Widely adopted in industry. Enterprise (most application servers, cloud backend software; cloud portal services); smart home: a broad variety of smart home solutions including DT QIVICON, devolo, AT&T Digital Life, Miele@Home etc.; telematics: various telematics solutions, including Groeneveld telematics solution for lorries, and MMLab telematics solutions for waste collection and cleaning services; adoption in AAL mainly in research projects (UniversAAL, sensiNact, etc.).
  - Development status: Release 6 Approved with planned revisions
  - Compliance: Formal certification process, reference implementations and compliance tests
  - Openness: Open to public. Publicly available specifications with reference implementations and compliance tests. Various open source and commercial implementations exist and are adopted by the industry
  - Ratification process (how the standard is being approved?): Done by members and open for consultation from external parties

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
  - Syntactical interoperability:
    - Application modules deployed as Java code packaged in JAR files with additional metadata
    - Deployment of native binaries using standard API.
    - Interaction with external devices through a unified abstraction layer

  - Technical interoperability
    - Management via HTTP/REST
    - Application modules deployed as Java code packaged in JAR files with additional metadata

        - Runtime interoperability with any Java Virtual Machine language that has Java bindings (e.g. Java, Scala, EcmaScript), and native code via JNI.
    - Semantic interoperability
        - Possibility of expressing relevant semantics via OSGi's Requirements / Capabilities model.

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs
    - The OSGi specifications provide a standardised service platform for interacting with services (both local and remote) using a variety of defined communication and messaging protocols, including UPnP, TR069, enOcean, OMA DM, HTTP/REST, JSON-RPC and many others built by the community

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative
    - The Strategic members of the OSGi Alliance include: Adobe, Deutsche Telekom, IBM, Liferay, NTT, Oracle, Paremus, ProSyst Software, Salesforce.com and Software AG. Numerous other companies are active contributing members , such as Orange, Telecom Italia, Sagemcom, Schneider Electric, Hitachi, NEC and Eclipse Foundation
    - OSGi Alliance liaises with various organizations. A collaboration between HGI, BBF, UPnP Forum and OSGi Alliance resulted in end-to-end service specifications for CPEs; Open Source communities such as Eclipse Foundation and Apache Foundation offer various reference implementations for OSGi specifications; EnOcean collaborates with the OSGi Alliance; other liaisons in IoT not be publicly announced yet, but very soon.

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
    - OSGi is being adopted in B2B and B2C product solutions, specifications are available for Smart Home, Enterprise, automotive, and mobile environments. An IoT Working Group has recently been established.

- Application area:
    - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
        - OSGi Alliance provides a horizontal platform with API's and device abstraction for specific vertical markets; it also provides specifications for enterprise solutions (app servers; cloud product solutions) and a framework for modular web application development

- Scope: mapping to knowledge areas of concerns in IoT.
    - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):
        - Communication and Connectivity knowledge area*:*
            - Gateway based architecture, interconnection of devices and the cloud.

- Integration/Interoperability knowledge area:
  - OSGi Alliance provides a device abstraction layer and various APIs for providing common access to external resources (both physical hardware and external services)

    The OSGi Framework provides a Java execution environment capable of supporting existing Java applications on small embedded systems, or large server hardware.

- Applications knowledge area:
  - OSGi Alliance provides a dynamic lifecycle management layer and standardised API that allows users to remotely install, manage, configure and update software components
  - The OSGi Alliance provides enRoute, a framework for modular development of web applications using OSGi best practices.
  - Numerous tools for dependency management and resource access exist
  - Configuration is able to be pushed to OSGi modules via a common interface, independent of how the configuration is stored.

- Infrastructure knowledge area:
  - OSGi Alliance provides specifications for large-scale enterprise deployments, embedded systems, and edge devices

- Devices and sensor technology knowledge area:
  - The OSGi specifications provide dynamic lifecycle management for modules and services, meaning that devices sensors can be dynamically added, removed, discovered, or updated within a running system.
  - Dynamic configuration management is provided for application and infrastructure modules allowing them to be updated without restarting the system.
  - A wide variety of operating platforms are supported. The core requirement is for a Java Virtual Machine implementation.

- Security and Privacy knowledge area:
  - The OSGi specifications include native support for trusted modules, and permission-based access to resources and services.
  - Permissions can be dynamically changed at runtime based on configuration.

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy
  - OSGi specifications are royalty free

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software
  - Publicly available specifications with reference implementations and compliance tests

- Various open source and commercial implementations exist and are adopted by the industry

5.2.16 Weightless

- Description:
  - A standard for wide area wireless IoT connectivity enabling low-power devices. Covers layers 1-3 of the OSI model.

- Readiness:
  1. Adoption (users base)
     - Reference implementations
  2. Development Status
     - Approved with planned revisions
  3. Compliance
     - Formal certification process
  3. Openness
     - Open by formal membership
  5. Ratification process (how the standard is being approved?)
     - Closed process done by members only with no consultation from external parties

- Interoperability level:
  - Technical interoperability

- Standards: Original standard developed by Weightless

- Supporting organizations : N/A

- Domain: Already correctly positioned in this figure.

- Application area: Horizontal connectivity layer.

- Scope: mapping to knowledge areas of concerns in IoT.
  - Communication and Connectivity knowledge area*:*

- IPR Policy Available:
  - FRAND with options for zero-royalty on the terminal side, all members required to agree.

- Specification Access:
  - Specification available only to members.

5.2.17 WWRF (Wireless World Research Forum)

- Description: main objective and focus of initiative
  - WWRF's goal is to encourage global research that will achieve unbounded communications to address key societal challenges for the future. The term "Wireless World" is used in a broad sense to address the support of innovation and business, social inclusion and infrastructural challenges. This will be achieved by creating a range of new technological capabilities from wide-area

networks to short-range communications, machine-to-machine communications, sensor networks, wireless broadband access technologies and optical networking, along with increasing intelligence and virtualization in networks. This will support a dependable future Internet of people, knowledge and things and the development of a service universe.

Features: high level functionalities covered by the initiative

- User needs and requirements
- Services, devices and service architectures
- Communication architectures and technologies
- Radio communication technologies

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.
  1. Adoption (users base)
     - No implementations
  2. Development Status
     - Under development
  3. Compliance
     - Not managed
     -
  4. Openness
     - Open by formal membership
     - Open to public (contributions and meeting attendance open to non-members)
  5. Ratification process (how the standard is being approved?)
     - Closed process done by members only with no consultation from external parties (WWRF does not produce standards, but white papers and other publications approved by Steering Board)

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
  - Standards are not developed by WWRF, so no interoperability level applies
- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs
  - WWRF does not produce standards or protocols, but produces white papers and technology overviews that provide information to SDO partners such as ITU-R and ETSI

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative
  - Nokia, Huawei and China Mobile are sponsors, other members include: Qualcomm, Fujitsu, Bell Canada, Sagem, HP, NEC, Ericsson, Intel, LG, DoCoMo

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
    - WWRF covers all these areas, so a position close to the centre is appropriate

- Application area:
    - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
        - Horizontal/Telecommunication

- Scope: mapping to knowledge areas of concerns in IoT.
    - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):
        - Communication and Connectivity knowledge area:
        - Applications knowledge area:
        - Infrastructure knowledge area:

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy
    - WWRF IPR Policy is included in the Articles of Association (http://www.wwrf.ch/files/wwrf/content/files/Membership/AoA_WWRF_revision_2015_revision%20F1.pdf). All IPR generated by members remains with members, WWRF does not seek to own IPR other than copyright of publications and registration of trademarks.

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software
    - Published WWRF white papers and other documents are available at http://www.wwrf.ch/publications.html
    - Draft documents are available to members at http://www.wwrf.ch/member-pages.html

5.3 IoT OSS Initiatives

This section provides a brief description of the IoT OSS initiatives mentioned in Section 3. These brief descriptions are following and are based on the OSS template described in Section 5.1.

The official URLs of each of these initiatives can be found via Table 6.

Table 6: OSS initiatives and their Official URLs

Initiative	URL
AllJoyn	https://allseenalliance.org/developers
Apache Spark	https://spark.apache.org
Arduino:	https://www.arduino.cc/
Contiki	http://www.contiki-os.org/
EclipseIoT	http://iot.eclipse.org/
Fi-ware	www.fiware.org
IoTivity	https://www.iotivity.org/
InfluxDB	https://influxdb.com/
LinuxIoTDM	https://wiki.opendaylight.org/view/IoTDM:Main
Mosquitto	https://projects.eclipse.org/projects/technology.mosquitto
Node-RED	http://nodered.org
OpenIoT	https://github.com/OpenIotOrg/openiot
openHAB	http://www.openhab.org/
OM2M	http://www.eclipse.org/om2m/
ONOS	http://onosproject.org/
OPFNV	https://www.opnfv.org
OpenDaylight	https://www.opendaylight.org/
OpenRemote	http://www.openremote.com/
OpenStack	https://www.openstack.org/
OpenWSN	https://openwsn.atlassian.net/wiki/pages/viewpage.action?pageId=688187
OWASP (Open Web Application Security Project)	https://www.owasp.org/
Particle (formally Spark)	http://spark.github.io/
Paho	http://www.eclipse.org/paho/
Riot: Real time OS for sensor networks	http://www.riot-os.org/
ROS (Robot Operating System)	http://www.ros.org/
SensiNact	http://open-platforms.eu/library/butler-smart-gateway
Sofia2	http://sofia2.com/home_en.html
ThingSpeak	https://thingspeak.com/
UniverSaal	http://www.universaal.org

5.3.1 IoTivity

- Description:
  IoTivity is an Open Source Project sponsored by the Open Interconnect Consortium (OIC) and hosted by the Linux Foundation. The aim of this project is to develop an open source software framework to seamlessly connect the billions of devices in the emerging Internet of Things (IoT), across multiple operating systems and network protocols.

  The founders of the OIC believe that both an industry standard specification and an open source implementation are necessary to drive true interoperability across these IoT devices. Moreover, the founders believe that true innovation can only happen when multiple parties come together, developing the source code in an open form, under open source governance rules.

OIC have released 1.0 standard specification. At the same time, the IoTivity project will release a full open source implementation of that specification. However, you can get started today by downloading and exploring the current release, and start contributing.

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.

    1. Community
        - Formal consortium
    2. Commitment
        - Dedicated committers from organizations
    3. Road map:
        - Formal road map
    4. Alignment of ongoing Standards
        - OSS output is aligned with SDO specifications - OIC
    5. Licensing
        - Apache License version 2.0.
    6. Portability
        - Multiple platforms are developed by project

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
    - Organisational interoperability. Note work is ongoing to interoperate through the OneM2M platform as well as across the OIC ecosystem

- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs
    - OIC

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative
    - OIC

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
    - Multiple domains – initial release has a consumer focus with a mix of connectivity and services.

- Application area:
    - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2
        - Different specifications cover different areas. The initial focus is on Smart Home

- Scope: mapping to knowledge areas of concerns in IoT.
  - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):

    - Communication and Connectivity knowledge area:
    - Integration/Interoperability knowledge area:
    - Applications knowledge area:
    - Infrastructure knowledge area:
    - IoT Architecture knowledge area:
    - Devices and sensor technology knowledge area:
    - Security and Privacy knowledge area:

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy
  - FRAND – Free licensing

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software
  - Code open on IoTivity web site – free to access for all - https://www.iotivity.org/

5.3.2 OM2M (Open platform for M2M)

- Description:
  OM2M (Open platform for M2M) is an open source implementation of the SmartM2M standard and OneM2M standard diffused by Eclipse foundation. The project is initiated by LAAS-CNRS. It provides a horizontal M2M service platform for developing services independently of the underlying network, with the aim to facilitate the deployment of vertical applications and heterogeneous devices.

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2); For each criterion please select one or more options.
  1. Community
     - Multiple organizations
  2. Commitment
     - Multiple volunteer committers
  3. Road map:
     - Frequent but non planned releases (small extension)
     - Planned releases (synchronization with standard)
  4. Alignment of ongoing Standards
     - SmartM2M (OM2M version 0.8)
     - OneM2M (OM2M version 1.0)
  5. Licensing
     - Eclipse Public License (ou EPL)
  6. Portability
     - Platform independent

- Interoperability level:

- Syntactical interoperability

- Standards:
  - OneM2M - OneM2M consortium
  - SmartM2M – ETSI

- Supporting organizations (mainly for Alliances/OSS):
  - LAAS-CNRS
  - Eclipse foundation

- Domain:
  - OM2M creates horizontal service and allows to create applications. It concerns B2C and B2B.

- Application area:
  - OM2M creates a complete IoT solutions for horizontal industry. Several companies and research laboratories use OM2M in different domains: smart-building, transportation, healthcare, energy and smart cities.

- Scope: mapping to knowledge areas of concerns in IoT.
  - Integration/Interoperability knowledge area:
  - IoT Architecture knowledge area:
  - Security and Privacy knowledge area:

- IPR Policy Available:
  - Eclipse Public License (ou EPL)

- Specification Access:
  - http://eclipse.org/om2m

5.3.3 sensiNact (aka BUTLER platform)

- Description:
  - sensiNact (aka BUTLER platform) is a horizontal IoT platform issued from the large scale FP7 project on IoT, BUTLER (~20 partners, 15M€ budget). The platform provides an abstraction layer underlying heterogeneous IoT ecosystem and provides common APIs and allow developers focusing on the business logic instead of underlying IoT technologies (communication, routing, device OS, etc.). Support for various IoT protocols and platforms is provided.

    Features: high level functionalities covered by the initiative
    - Generic APIs providing homogeneous access to underlying IoT devices and platforms; not only sensing but also actuating.
    - Support for various southbound IoT protocols and platforms (CoAP, Zigbee, enOcean, KNX, Xbee, Sigfox, NFC, BLE, MQTT, XMPP, FIWARE, etc.)
    - Support for various northbound remote access protocols (HTTP REST, JSON-RPC, OneM2M, OMA LWM2M, CDMI, NGSI etc.)
    - Platform as a Service providing easy deployment and management of IoT application and services
    - Complex Event Processing engine for fusion of events from various sensors

- Tools and libraries for developers for rapid prototyping of IoT applications

- Readiness: (for OSS, use Table 1, for SDO/Alliances, use Table 2)
  sensiNact is a relatively new born initiative which is around the level 1-2 of readiness in the table, that will rapidly reach to level 2 - 3
  - Community: currently mostly one single organization (CEA) is the main contributor + contributions from ongoing EU project partners.
  - Commitment: Formally appointed committers from CEA + multiple volunteer committers from ongoing EU projects
  - Roadmap: Regular planned releases
  - Alignment of ongoing Standards: Support for various IoT standards (see above), active participation to standardization (e.g., OSGi)
  - Licensing: Apache Software License 2.0
  - Portability: multiple platforms are developed by project

- Interoperability level: identify the interoperability levels considered by the SDO/Alliance/OSS initiative, see Appendix A for details:
  - Syntactical interoperability
    - Defines device/service/resource model serialized in JSON format
  - Technical interoperability
    - Provides interoperability among various IoT protocols and platforms (CoAP, Zigbee, enOcean, KNX, Xbee, Sigfox, NFC, BLE, MQTT, XMPP, FIWARE,
  - Semantic interoperability
    - Possibility of extending the resource model with semantics capabilities (e.g. JSON-LD).
  - Organisational interoperability
- Standards: standards and protocols proposed (SDO/Alliance) or supported (Alliance/OSS); Include details on whether an SDO/Alliance specified original protocols, or whether they are using and integrating standards and protocols developed by other SDOs
  - Supported standards: CoAP, Zigbee, enOcean, KNX, NFC, BLE, MQTT, XMPP, OMA NGSI, OMA LWM2M, OneM2M, CDMI
  - Leveraging the OSGi standard

- Supporting organizations (mainly for Alliances/OSS): main organizations that back the initiative
  - CEA is the main organization + several industrial and academic partners providing their support.

- Domain: position the initiative, with respect to the four quadrants, see Figure 1 in Section 2, related to the market domain (consumer/industrial internet –horizontal axis) and the technical domain (connectivity, service&applications – vertical axis);
    - sensiNact is a platform for managing IoT services & applications. It is domain agnostic and can be applied to consumer or industrial business.

- Application area:
    - whether the SDO/Alliance/OSS (or the WG/TC) initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, or whether it is focusing on a particular vertical industry (e.g., Smart City), when applicable, see Figure 2 in Section 2

- sensiNact is focusing the horizontal industry, a plug&play application platform for various IoT vertical domains. Deployments in smart home, smart office, smart transportation, and smart city have already been done.

- Scope: mapping to knowledge areas of concerns in IoT.
  - The identified knowledge areas are (Note that an initiative can be mapped to more than one knowledge areas):
    - Communication and Connectivity knowledge area*:*
      - covers mainly specification of communication protocol layers, e.g., PHY, MAC, NWK, Transport, Application layer, and their types, e.g., Wireless/Radio and Wireline; *it could also include management associated with the connectivity area*
      - sensiNact provides protocol bridges for various communication protocols (Zigbee, KNX, enocean, MQTT, XMPP, CoAP, etc.)
    - Integration/Interoperability knowledge area:
      - covers mainly specification of common IoT features required to provide integration and interoperability
      - sensiNact's main knowledge area is integration since it provides a platform integration various IoT devices and exposing their functionalities in terms of sensing and actuating services. It allows interoperability among those devices on top of which applications from vertical domains can be built.
    - Applications knowledge area:
      - covers the support of the applications lifecycle including development tools/models, deployment and management; *including Analytics, application supporting tools and application domain specific activities*
      - sensiNact provides SDK and tool for IoT application development, deployment and run-time management
    - Infrastructure knowledge area:
      - covers aspects such as SDN, cloud computing, Mobile Edge Computing (MEC), fog computing, and other infrastructure topics, leaving all topics related "only" to communications in the connectivity knowledge area; *it could also include management associated with the at the infrastructure level*
    - IoT Architecture knowledge area:
      - covers integrated/complete IoT specification solutions, including architecture descriptions
      - sensiNact is based on the BUTLER architecture, which shares commonalities with the IoT-A architecture (device/service/resource model)
    - Devices and sensor technology knowledge area:
      - covers mainly device/sensor lifecycles, including operating systems, platforms, configuration management, *sensor/actuators virtualization etc.*
      - sensiNact is agnostic to device and sensor technologies
    - Security and Privacy knowledge area:

    - covers security and privacy topics
    - Provides token based authentication and profile based authorization

- IPR Policy Available: mention if there is any IPR policy available (e.g., FRAND); if available include a reference to the description of this IPR policy
    - Apache Software License 2.0

- Specification Access: Describe whether and how SDO/Alliance/OSS members and non-members can get access to published and non-published (draft) specifications and/or software
    - First public information at http://open-platforms.eu/library/butler-smart-gateway/. Github repository under construction.

6. Appendix 2: Technology Trends for the Support of IoT

This section provides a brief description of technology trends for the support of IoT.

6.1 Wireless Connectivity Trends for the Support of IoT

Wireless communications are strongly regulated by National and International rules and directives. SDOs are allocating frequency bands with related radiated power and issuing standards on how technologies must comply to specific region's regulation.

There are several technologies used for connectivity for the support of IoT. Figure 6 shows the wireless connectivity trends, which is divided into four quadrants. The horizontal axis represents the device cost in terms of the supported bit rate and the vertical axis represents the wireless technology coverage range.
Please note that by using meshed technologies and topologies, the WPAN (Wireless Local Access Network) and WLAN (Wireless Personal Area Network) technologies can also be enabled to support a wider coverage e.g., Neighbourhood Area deployments. In case a wider coverage is needed, the range limit of the radio technologies could be overcome by using multiple access points/base stations and/or gateways that are geographically distributed and connected to a common backbone.
The depicted arrow in Figure 6 emphasizes that current developments in LTE standardization, e.g., Cellular IoT (CIoT), will enable the LTE technology to be used within low power consumption wireless devices.

Figure 6: Wireless Connectivity Trends

7. References

[ETSI-position] "ETSI White Paper No. 3: Achieving Technical Interoperability - the ETSI Approach", ETSI White paper, to be retrieved via:
http://www.etsi.org/images/files/ETSIWhitePapers/IOP%20whitepaper%20Edition%203%20final.pdf

[IERC-position] "Internet of Things, IoT Semantic Interoperability: Research Challenges, Best Practices, Recommendations and Next Steps", IERC white paper, to be retrieved via:
http://docbox.etsi.org/SmartM2M/Open/AIOTI/!!SemanticDev/20150724FirstTelcoSemanticDev/IERC_Position_Paper_IoT_Semantic_Interoperability_Final.pdf

Authors

Name	Company/Organisation	Email address
Georgios Karagiannis	Huawei	georgios.karagiannis@huawei.com
Howard Benn	Samsung	howard.benn@samsung.com
Werner Berns	Texas Instruments	Werner.Berns@ti.com
Angel Boveda	Wireless Partners	angel.boveda@wirelesspartners.es
Marco Carugi	NEC	marco.carugi@gmail.com
Pablo Chacin	SenseFields SL	pchacin@sensefields.com
John Davies	BT	john.nj.davies@bt.com
Thierry Demol	CITC-EuraRFID	tdemol@citc-eurarfid.com
Jean-Pierre Desbenoit	Schneider Electric	jean-pierre.desbenoit@schneider-electric.com
Zeta Dooly	Waterford Institute of Technology	zdooly@tssg.org
Omar Elloumi	Alcatel-Lucent	omar.elloumi@alcatel-lucent.com
Patrick Guillemin	ETSI	patrick.guillemin@etsi.org
Levent Gurgen	CEA	levent.gurgen@cea.fr
Juergen Heiles	Siemens	juergen.heiles@siemens.com
Sharadha Kariyawasam	HW Communications Ltd	sharadha@HWCOMMS.COM
Jochen Kilian	DSPG	jochen.kilian@dspg.com
Guenter Kleindl	ATOS	guenter.kleindl@atos.net
Paul Murdock	LANDIS+GYR	Paul.Murdock@LANDISGYR.COM
Thomas Paral	TE Industrial	thomas.paral@te.com
Nigel Rix	KTN: Knowledge Transfer Network	nigel.rix@ktn-uk.org
Friedhelm Rodermund	Vodafone	rodermund@vodafone.de
Mohammad-Reza Tazari	Fraunhofer IGD	saied.tazari@igd.fraunhofer.de
Martin Serrano	National University of Ireland Galway	martin.serrano@insight-centre.org
Carlos Ralli Ucendo	Telefonica	carlos.ralliucendo@telefonica.com
Ovidiu Vermesan	SINTEF	Ovidiu.Vermesan@sintef.no
Alexander Vey	IBM	VEY@de.ibm.com
Patrick Wetterwald	CISCO	pwetterw@cisco.com

Reviewers:

Patrick Guillemin, WG3 Chair, ETSI, France
Jean-Pierre Desbenoit, WG3 alternate Chair, Schneider Electric, France

Acknowledgements

The AIOTI would like to thank the European Commission services for their support in the planning and preparation of this document. The recommendations and opinions expressed in this document do not necessarily represent those of the European Commission. The views expressed herein do not commit the European Commission in any way.

© European Communities, 2015. Reproduction authorised for non-commercial purposes provided the source is acknowledge.