Alliance for IoT and Edge Computing Innovation

IoT LSP Standard Framework Concepts

Release 3.0

AIOTI WG Standardisation

February 2023

Executive Summary

This deliverable is an updated version of the Release 2.9 and 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 Content

Executive Summary 2

Table of Figures 5

List of Tables 6

1. Goal and Motivation 7

2. IoT SDO and Alliance Initiatives Landscape 8

3. IoT Open Source Software Initiatives Landscape 10

4. Mapping SDO/Alliance/OSS/ Initiatives into Knowledge Areas 11

5. Appendix 1: IoT SDOs, Alliances and OSSs 14

5.1 SDO, Alliance, and OSS Initiatives Template for Information Collection 14

5.2 IoT SDO/Alliance Initiatives 18

5.2.1 3GPP (3rd Generation Partnership Project) 21

5.2.2 AVNU Alliance 23

5.2.3 BBF (Broadband Forum): Broadband User Services (BUS) Work Area 24

5.2.4 European Centre for Certification and Privacy (ECCP) 27

5.2.5 ESMIG 28

5.2.6 ETSI (European Telecommunications Standards Institute) 29

5.2.7 Fairhair 55

5.2.8 GlobalPlatform 56

5.2.9 GS1 58

5.2.10 GSMA (GSM Association) 60

5.2.11 HyperCat 61

5.2.12 IEC (International Electrotechnical Commission) 62

5.2.13 IEEE Standards Association 66

5.2.14 IEEE P2413: Standard for an Architectural Framework for the Internet of Things 67

5.2.15 IEEE P2874 SPATIAL WEB Protocol, Architecture and Governance Working Group 68

5.2.16 IETF (Internet Engineering Task Force) 69

5.2.17 IRTF (Internet Research Task Force) 87

5.2.18 International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) 92

5.2.19 ISO/IEC JTC1 95

5.2.20 M2.COM 98

5.2.21 MIPI Alliance 99

5.2.22 NFC (Near Field Communication) Forum 102
5.2.23 OCF (Open Connectivity Foundation) 103
5.2.24 OneM2M 104
5.2.25 OSGi Alliance 107
5.2.26 The Open Group / Open Platform 3.0 110
5.2.27 TMForum 113
5.2.28 Weightless 116
5.2.29 UDG Alliance 117
5.2.30 World Wide Web Consortium (W3C) 118
5.2.31 WWRF (Wireless World Research Forum) 121
5.3 IoT OSS Initiatives 123
5.3.1 Matter 124
5.3.2 Civil Infrastructure Platform (CIP) 125
5.3.3 Eclipse IoT-Testware 126
5.3.4 IoTivity 128
5.3.5 IoT6 130
5.3.6 OM2M (Open platform for M2M) 131
5.3.7 sensiNact (aka BUTLER platform) 132
5.3.8 Sofia2 134
5.3.9 UniversAAL IoT 137
5.3.10 Warp10 from Cityzen Data 139
6. Appendix 2: Technology Trends for the Support of IoT 141
6.1 Wireless Connectivity Trends for the Support of IoT 141
References 142
Editor and Contributors 143
Acknowledgements 145
About AIOTI 146

Table of Figures

Figure 1: IoT SDO and Alliances Landscape **8**
Figure 2: IoT SDO and Alliance Initiatives Projection on Vertical and Horizontal Domains **9**
Figure 3: IoT OSS Initiatives Landscape **10**
Figure 4: Mapping of IoT SDO and Alliance Initiatives into Knowledge Areas; **12**
Figure 5: Mapping of IoT OSS Initiatives into Knowledge Areas **13**
Figure 6: Wireless Connectivity Trends **141**

List of Tables

Table 1: OSS Readiness Criteria and Options **16**

Table 2: SDO/Alliance Readiness Criteria and Options **17**

Table 3: SDO/Alliance initiatives and their Official URLs: Part 1 ..... **18**

Table 4: SDO/Alliance initiatives and their Official URLs: Part 2 ..... **19**

Table 5: SDO/Alliance initiatives and their Official URLs: Part 3 ..... **20**

Table 6: OSS initiatives and their Official URLs **123**

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 is an updated version of the Release 2.9 and gives several ways of visualising the landscape in order to simplify and facilitate the usage of the information in various IoT application domains. AIOTI WG Standardisation 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 WG Standardisation and relevant initiatives as well as on the collected information presented in Appendix 1 (Section 5).

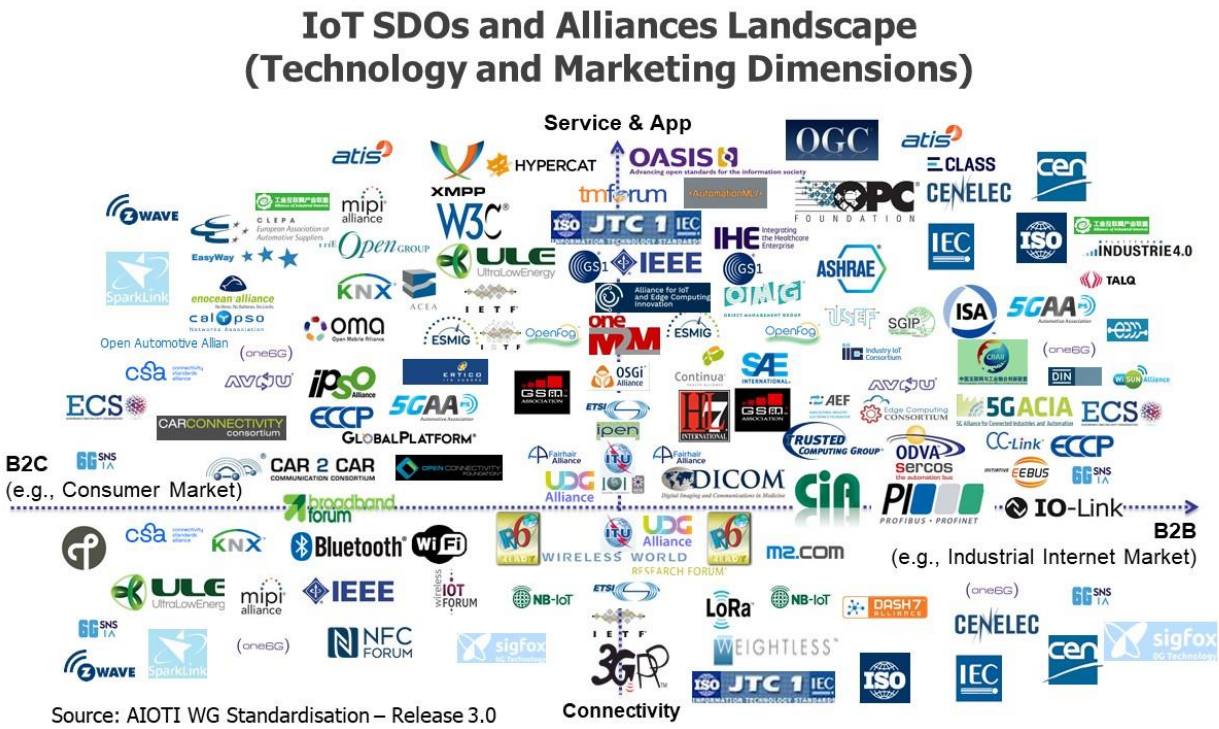


Figure 1: IoT SDO and Alliances Landscape

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 at highlighting 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".

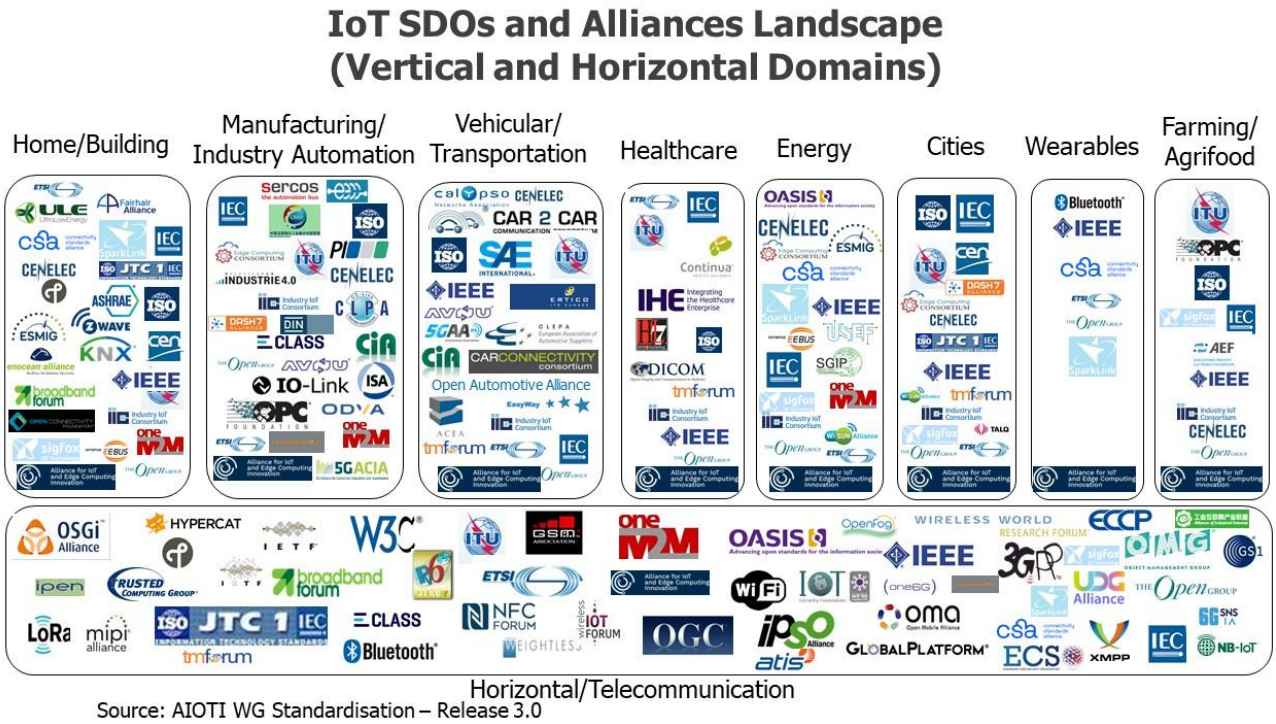


Figure 2: IoT SDO and Alliance Initiatives Projection on Vertical and Horizontal Domains

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.

However, it has 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 WG Standardisation 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.

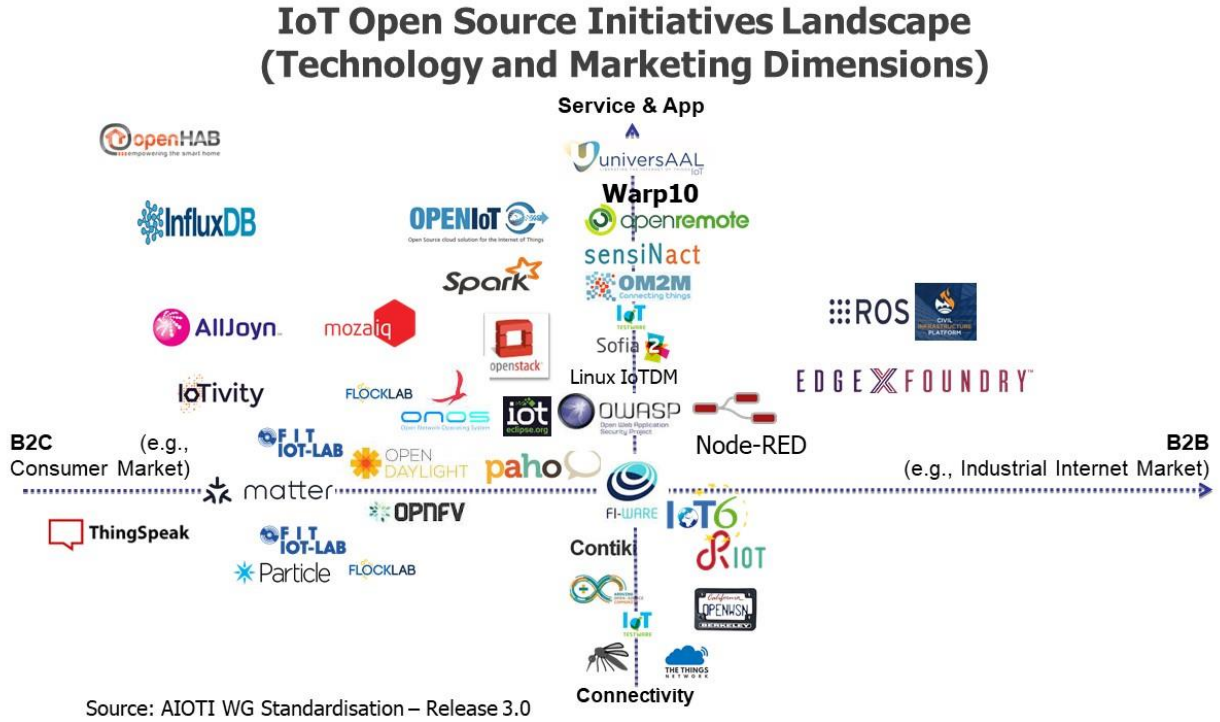


Figure 3: IoT OSS Initiatives Landscape

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 WG Standardisation and as well in the relevant initiatives and on the collected information presented in Appendix 1 (Section 5).

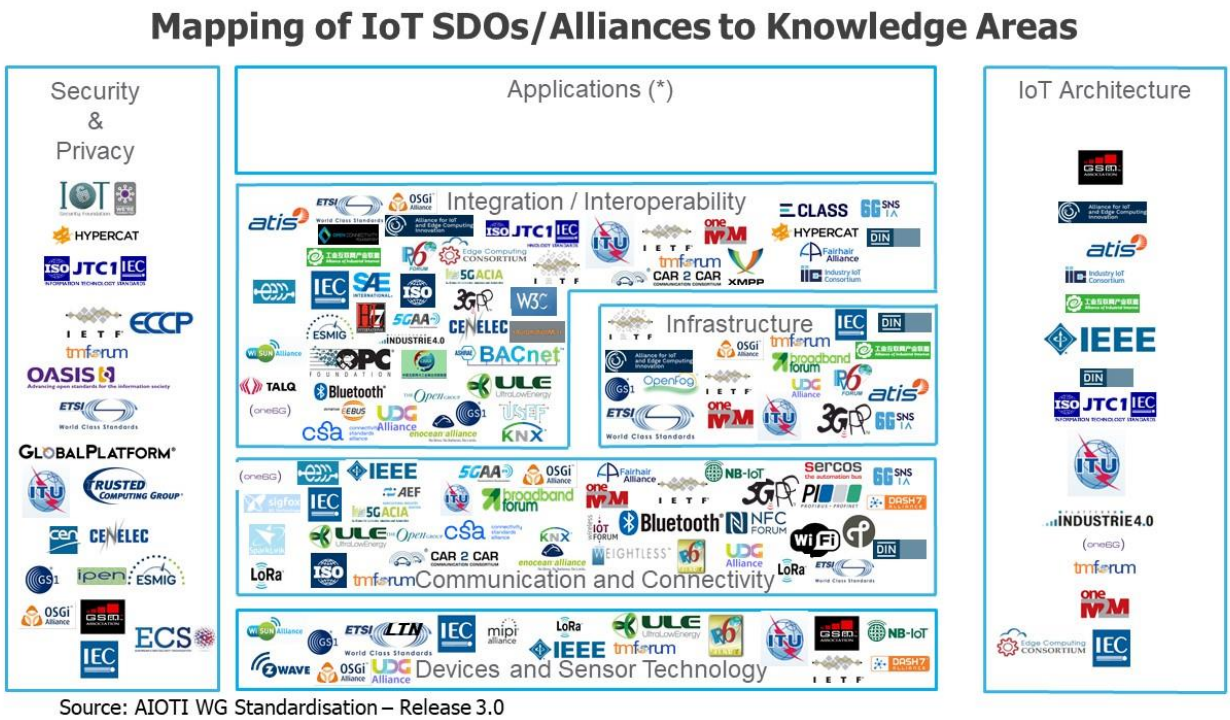
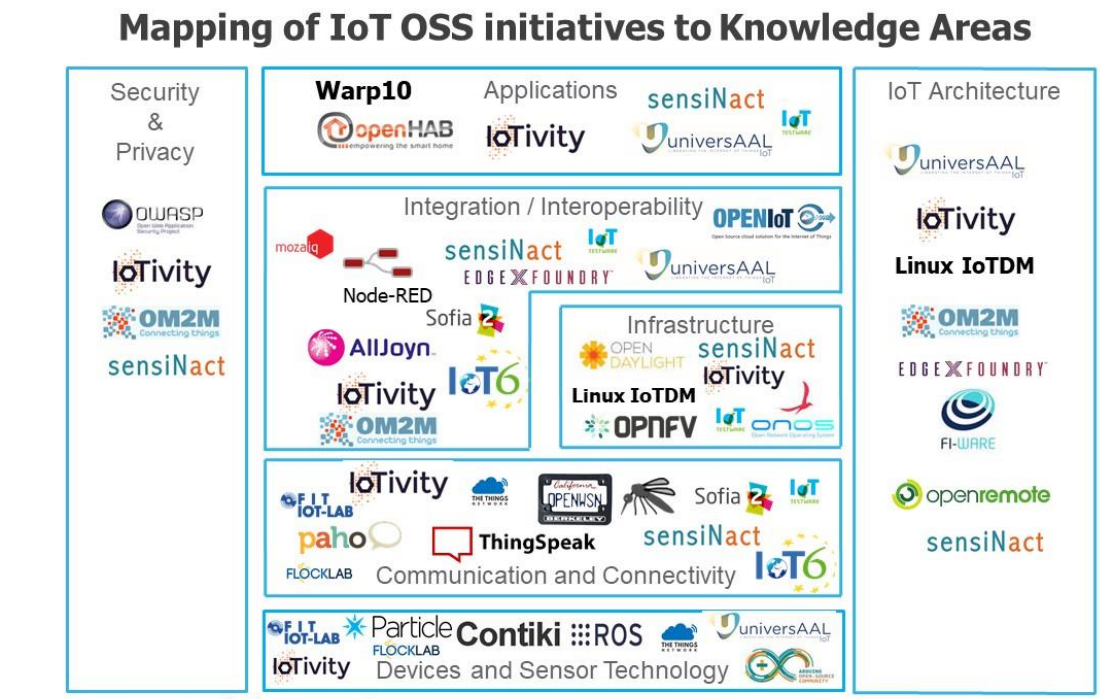


Figure 4: Mapping of IoT SDO and Alliance Initiatives into Knowledge Areas

(*) A large number of initiatives shown in Section 2 that focus on vertical domains, can be mapped to the Application knowledge area



Source: AIOTI WG Standardisation – Release 3.0

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 WG Standardisation 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 [IERC-position], [ETSI-position] and 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 and 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 already 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, XML or JSON.

- 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/
5GAA (5G Automotive Association)	http://www.5gaa.org/
5G-ACIA (5G Alliance for Connected Industries and Automation)	https://www.5g-acia.org/
6G Smart Networks and Services Industry Association (6G-IA)	https://6g-ia.eu/
ACEA (European Automobile manufacturing Association):	http://www.acea.be/
AEF (Agricultural Industry Electronics Foundation)	http://www.aef-online.org/
Alliance of Industrial Internet	http://en.aii-alliance.org/
AIOTI (Alliance for IoT and Edge Computing Innovation)	http://www.aioti.eu/
Allseen Alliance	https://allseenalliance.org/
ASHRAE	https://www.ashrae.org/
ATIS	http://www.atis.org
Automation ML	https://www.automationml.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/
CSA (Connectivity Standards Alliance)	https://csa-iot.org/
DASH7	https://www.dash7-alliance.org/
DICOM (Digital Imaging and Communications in Medicine)	http://dicom.nema.org/
DIN	https://www.din.de/en
easyway	https://www.easyway-its.eu/
EEBUS	https://www.eebus.org/
ECLASS	http://www.eclass.de/
EECC (European Edge Computing Consortium)	https://ecconsortium.eu/
ECC (Edge Computing Consortium)	http://en.ecconsortium.org/

Initiative	URL
ECCP (European Centre for Certification and Privacy)	www.eccpcentre.org
ECSO (European Cyber Security Organisation):	http://www.ecs-org.eu/
ERTICO - ITS Europe	http://ertico.com/
ESMIG	http://esmig.eu/
ETSI (European Telecommunications Standards Institute)	http://www.etsi.org/
Enocean Alliance	https://www.enocean-alliance.org/
GlobalPlatform	http://www.globalplatform.org/

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

Initiative	URL
GSMA	http://www.gsma.com/
GS1 (Global Standards 1)	http://www.gs1.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 (Industry IoT Consortium)	https://www.iiconsortium.org/
IPEN (Internet Privacy Engineering Network)	https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/IPEN
IPSO (Internet Protocol for Smart Object)	http://www.ipso-alliance.org/
IPv6 Forum	http://www.ipv6forum.com/
IRTF (Internet Research Task Force)	http://www.3gpp.org/
IO-Link	http://www.io-link.com/
IoT Security Foundation	https://www.iotsecurityfoundation.org/
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/
M2.COM	http://www.m2com-standard.org/
MIPI Alliance	http://mipi.org/
NB-IoT Forum	http://www.gsma.com/connectedliving/narrow-band-internet-of-things-nb-iot/
NFC Forum	http://nfc-forum.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
Open Connectivity Forum	http://openconnectivity.org/
ODVA	https://www.odva.org/
OGC (Open Geospatial Consortium)	http://www.opengeospatial.org/
OMA (Open Mobile Alliance)	http://openmobilealliance.org/
One6G	https://one6g.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/
Sigfox	https://www.sigfox.com/
SGIP (Smart Grid Interoperability Panel)	http://sgip.org/
Sparklink	http://www.sparklink.org.cn/en/
TALQ	https://www.talq-consortium.org/
Thread group	http://threadgroup.org/
TMForum	https://www.tmforum.org/
Trusted Computing Group	http://www.trustedcomputinggroup.org/
UDG Alliance	https://www.udgalliance.org/
USEF (Universal Smart Energy Framework)	https://www.usef.energy/
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/
WI-SUN Alliance	https://wi-sun.org/
Z-Wave®	https://www.z-wave.com/
XMPP	http://xmpp.org/

5.2.1 3GPP (3rd Generation Partnership Project)

- Description:

The below text is 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, providing 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:

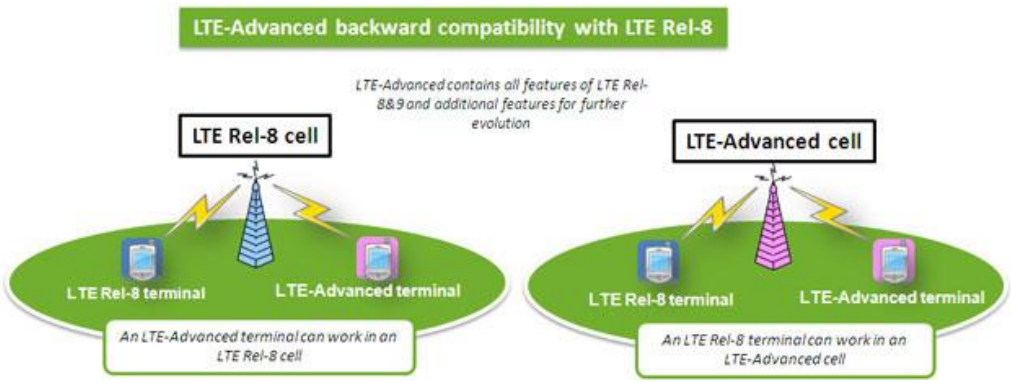
- Radio Access Networks (RAN);
- Service & Systems Aspects (SA),
- Core Network & Terminals (CT);
- GSM EDGE Radio Access Networks (GERAN).

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:

1. Adoption:
   - 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:

- Done by members and open for consultation from external parties.

- Interoperability level:
  - Technical interoperability.
  - Organisational interoperability.
- Standards:

1. As referred above 3GPP covers cellular telecommunications network technologies, including radio access, the core transport network, and service capabilities, including work on codecs, security and quality of service and providing 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:

  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:
  - 3GPP provides network connectivity along the entire horizontal axis and mainly in vertical axis part under the horizontal axis.
- Application area:
  - 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.
- IPR Policy Available:

2. http://www.3gpp.org/about-3gpp/legal-matters
3. http://www.3gpp.org/ftp/Information/Working_Procedures/3GPP_WP.htm#Article_55
4. http://www.3gpp.org/ftp/Inbox/2008_web_files/3gppagre.pdf

- Specification Access:
  - 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, see www.avnu.org.
- Readiness:

1. Adoption:
   - 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:
   - Done by members and open for consultation from external parties.

- Interoperability level:
  - Technical interoperability.
- Standards:
  - Certification procedures based on Open standards (IEEE 802.1TSN, 802.1 series, IEEE 1588, IETF DetNet…).
- Supporting organizations
  - Leader in:
    - Automotive.
    - Industrial automation.
    - Audio / video.
- Domain:
  - Automotive.
  - Industrial automation.
  - Audio / video.
- Application area:
    - Smart manufacturing
    - Automotive
    - Audi / Video
- Scope:
  - 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:
  - FRAND (http://avnu.org/wp-content/uploads/2014/05/AVnu-Alliance-IPR-Policy.pdf).
- Specification Access:
  - 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:
  1. Adoption:
     - 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:
     - Closed process done by members only with no consultation from external parties.
- Interoperability level:

- Syntactical interoperability.
- Technical interoperability.

- Standards:
  - 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.

  5. 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:

  6. https://www.broadband-forum.org/cwmp.php.
  7. https://www.broadband-forum.org/cwmptools.php.

- Supporting organizations:
  - BUS is a BBF Work Area.

- Domain:
  - 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 and applications.

- Application area:
    - 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:
    - 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:
    - 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 European Centre for Certification and Privacy (ECCP)

- Description:

  ECCP (www.eccpcentre.org) has been established to support the development and maintenance of standards related to data protection and ICT. One of its mission is to maintain the Europrivacy certification scheme (www.europrivacy.org) for certifying GDPR compliance. Europrivacy has been developed through the European research programme to be applicable to IoT deployments and emerging technologies such as artificial intelligence, smart grids, connected vehicles, eHealth, smart cities, distributed ledger technologies. ECCP is also working on ICT certification standards for IoT.

- Readiness:

  1. Adoption:
     - Europrivacy certification scheme has been endorsed by major certification bodies, consulting firms and law firms.

  2. Development Status:
     - Approved, with regular updates.

  3. Compliance
     - With ISO standards and the European General Data Protection Regulation (GDPR) as well as national regulations, including non-European regulations.

  4. Openness
     - Made available through free licensing to qualified companies.

  5. Ratification process:
     - Through consultation with data protection experts and supervisory authorities. Maintained and supervised by an international board of experts in data protection.

- Interoperability level:
  - Regulatory compliance with European and non-European regulations in data protection. Interoperable with ISO/IEC 17065 and 17021-1 certification processes, as well as with ISMS certification process such as ISO/IEC 27001 and 27701. Applicable to all IoT domains.

- Standards:
  - Europrivacy for data protection and GDPR compliance certification.

- Supporting organizations:
  - Universities, research centres, certification bodies, law firms, consulting firms, and close cooperation with the national supervisory authorities.

- Domain:
  - Applicable to all data processing, including consumer and industrial IoT.
  - Mainly focused on the application layer (data), but addresses also lower layers for security management.

- Application area:
  - ECCP is fully cross-domain, encompassing e-health, smart buildings, smart cities, smart factories, supply chains, smart agriculture, smart grid, etc.

- Scope:
  - Data protection, regulatory compliance (GDPR, NIS, ePrivacy, etc.) and certification.

- IPR Policy Available:
  - IPR is managed by ECCP and made available through free licensing to qualified service providers.

- Specification Access:
  - Accessible through the Europrivacy community website

5.2.5 ESMIG

- Description:
  - ESMIG represents European companies that provide products, information technology and services for multi-commodity metering, display and management of energy consumption at consumer premises
  - Features: high level functionalities covered by the initiative
- Readiness:
  1. Adoption:
     - Widely adopted in industry.
  2. Development Status:
     - Approved with planned revisions.
  3. Compliance:
     - Having compliance testing process (include test suites, method, etc.)
  4. Openness:
     - Open by formal membership.
  5. Ratification process:
     - Open process for all parties interested in the ratification.
- Interoperability level:
  - Organisational interoperability.
- Standards:
  - ESMIG does not develop specifications, but is advocating open standards use.
  - The standards that ESMIG supports are listed in the Smart Meters Coordination Group report, starting with CEN/CENELEC/ETSI TR 50572 and updated on yearly basis in a CEN/CENELEC/ETSI workplan.
  - These specifications cover broad area from communication technologies, security and application related protocols which are used in smart energy distribution systems for metering and consumer energy management.
- Supporting organizations:
  - ESMIG members are: Apator, Chameleon, Elgama-Elektronika, Elster, Ericsson, Gemalto, geo, Inepro, Iskraemeco, Itron, Janz, Kamstrup, Kisters, Landis+Gyr, Luna, Mpare, Networked Energy Services, Sagemcom, SAP, Secure Meters(UK), Sierra Wireless, Sigma Telas, Telit, u-blox, Vodafone, Watt-IS, Wirepas, ZIV.
- Domain:
  - Our member companies are working in energy distribution solutions from utilities to consumer premises. Hence ESMIG position itself as a service and application provides in B2B and B2C environment.
- Application area:
  - ESMIG is focusing to energy vertical
- Scope:
    - Integration/Interoperability knowledge area:
      - ESMIG is working in this area to ensure working smart energy distribution and delivery to consumers.
    - Infrastructure knowledge area:
      - ESMIG has a holistic understanding of the infrastructure for Energy measurement and management on energy distribution systems and their operation.
    - Devices and sensor technology knowledge area:
      - ESMIG members are developing equipment, such as smart electricity meters, communication solutions, data management systems and displays.
    - Security and Privacy knowledge area:
      - ESMIG has developed a recommendation for smart meters security.
- IPR Policy Available:
  - ESMIG does not have any IPR policy.
- Specification Access:
  - ESMIG uses available open standards by selected SDO or organizations when relevant.

5.2.6 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 (European Telecommunications Standards Institute) - a European Standards Organization with global impact (https://www.etsi.org/about/about-us)

  ETSI provides members with an open, inclusive and collaborative environment. This environment supports the timely development, ratification and testing of globally applicable standards for ICT-enabled systems, applications and services.

  ETSI is at the forefront of emerging technologies across all sectors of industry and society that make use of ICT. The ETSI 900+ member organizations are drawn from 64 countries and five continents.

  Some of the benefits of the ETSI membership include:

  - access to the most up-to-date information on global ICT standards
  - direct participation in standards development
  - competitive advantage through early standard adoption
  - opportunities to network with industry leaders

  ETSI operates on a not-for-profit basis and are one of only three bodies officially recognized by the EU as a European Standards Organization.

  A EUROPEAN STANDARDS ORGANIZATION

  ETSI is a European Standards Organization (ESO), being the recognized regional standards body dealing with telecommunications, broadcasting and other electronic communications networks and services.

  ETSI has a special role in Europe. This includes supporting European regulations and legislation through the creation of Harmonised European Standards. Only standards developed by the three ESOs (CEN, CENELEC and ETSI) are recognized as European Standards (ENs).

  ETSI GLOBAL IMPACT

  ETSI was initially founded to serve European needs, but it has a global perspective. ETSI standards are now used the world over.

  ETSI collaborates and works in partnership with different types of organizations around the world. This makes us well placed to support the ETSI members who operate in an increasingly international and competitive environment.

  In addition, ETIS is a partner in the international Third Generation Partnership Project (3GPP™). Through this project, ETSI is helping to develop 4G and 5G mobile communications. ETSI also works with partners around the globe in the oneM2M partnership project to develop standards for machine-to-machine communications.

- Readiness:

  1. Adoption:

     Widely adopted in industry.

  2. Development Status:

     Depends on group and specification.

  3. Compliance:

4. Openness:

Results and work programme are public. Most technical groups are open to ETSI members some (ISGs) are also open to ETSI non-members.

5. Ratification process:

Done by members and open for consultation from external parties.

- Interoperability level:
  - Organisational interoperability.
- Standards:
  - Depends on specification.
- Supporting organizations:
- Domain:
  - Multiple domains.
- Application area:
  - Different specifications cover different areas.
- IPR Policy Available:
  - FRAND – ETSI IPR Policy - http://www.etsi.org/about/how-we-work/intellectual-property-rights-iprs.
- Specification Access:
  - Specifications available to the public for free from the ETSI web site https://www.etsi.org/standards#Pre-defined%20Collections.

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) (TBs) 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, such as:

- 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.

Moreover, 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:

    1. Adoption:

        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:

        Done by members and open for consultation from external parties.

- Interoperability level:
    - Organisational interoperability.
- Standards:
    - Depends on specification.

- Supporting organizations:
    - Not relevant.
- Domain:
    - Multiple domains.
- Application area:
    - Different specifications cover different areas. Smart City focus in some specifications.
- Scope:
    - 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:
    - FRAND – ETSI IPR policy - http://www.etsi.org/about/how-we-work/intellectual-property-rights-iprs.
- Specification Access:
    - 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 ETSI TC CYBER will be performed in close co-operation with relevant standards activities within and outside ETSI.

These activities 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:

- ETSI 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:

- ETSI TC CYBER is in 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 ETSI 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:

1. Adoption:

   Widely adopted in industry.

2. Development Status:

   Depends on specification, some published others under development.

3. Compliance:

4. Openness:

   Results are open to the public – TC Cyber participation is only for ETSI members.

5. Ratification process:

   Done by members and open for consultation from external parties.

- Interoperability level:
  - Organisational interoperability.
- Standards:
  - Depends on specification.
- Supporting organizations:
  - Not relevant.
- Domain:
  - Multiple domains.
- Application area:
  - Different specifications cover different areas. Smart City focus in some specifications.
- IPR Policy Available:
  - FRAND – ETSI IPR Policy - http://www.etsi.org/about/how-we-work/intellectual-property-rights-iprs.
- Specification Access:
  - Specifications available to the public for free from the ETSI web site https://www.etsi.org/standards#Pre-defined%20Collections

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:
    1. Adoption:
        - 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:
        - Done by members and open for consultation from external parties.
- Interoperability level:
    - Complete technical interoperability from Physical layer to application layer.
- Standards:
    - 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:
    - 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:
    - The primary knowledge areas is Communication and Connectivity knowledge area.
    - An additional knowledge areas is Devices and sensor technology knowledge area.
- IPR Policy Available:
    - FRAND.
- Specification Access:
    - ETSI specifications are publicly available.

ETSI TC ERM

- Description:

  Three TC ERM TG28 work items are dealing with LTN (Low Throughput Networks). These work items are intended to define the radio interface and key architecture features of a Low Throughput Network (LTN), which is an acronym for low power wide area networks.

    - The first document (a TR) on use cases and system requirement is in early draft status.
    - The second document (a TS) on architecture is still under preliminary discussions. Its writing should start beginning of 2016.
    - The third document (a TS) on protocols and interface is also under preliminary discussions. As this TS will be quite long to produce, it has been decided to issue a first document with only the physical layer clauses. This first release is expected by end Q1 2016 and is aimed at silicon companies to help them to include LTN in their road-maps.

ETSI TC ERM TG28 / LTN	Full title/ short title
Doc. Nb. TS 103 358 Ref.DTS/ERM-TG28-504	ERM; Low Throughput Networks (LTN) Architecture / LTN architecture
Doc. Nb. TS 103 357 Ref.DTS/ERM-TG28-503	ERM Low Throughput Networks (LTN) Protocols for interfaces A, B and C / Protocols for LTN interfaces A, B and C
Doc. Nb.TR 103 249 Ver.0.0.2 Ref. DTR/ERM-TG28-505	ERM Low Throughput Network (LTN) Use cases and System Requirements / LTN use cases and Systems Requirements

The following published ETSI Group Specifications (created by ETSI ISG LTN) are referred in TC ERM/TG28 work:

- ETSI GS LTN 001: http://www.etsi.org/deliver/etsi_gs/LTN/001_099/001/01.01.01_60/gs_LTN001v010101p.pdf, LTN Use Cases.
- ETSI GS LTN 002: http://www.etsi.org/deliver/etsi_gs/LTN/001_099/002/01.01.01_60/gs_LTN002v010101p.pdf, Architecture Definition.
- ETSI GS LTN 003: http://www.etsi.org/deliver/etsi_gs/LTN/001_099/003/01.01.01_60/gs_LTN003v010101p.pdf, Protocols and Interfaces.

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 ETSI 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;
- ETSI 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 ETSI TC-RES, ETSI TC-ERM is the parent body for project oriented (vertical) radio equipment and system standardisation activities. ETSI TC-ERM, via designated Task Groups, provides ETSI with a range of deliverables for sundry radio equipment and systems. ETSI 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

- ETSI 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.

Some of the published documents are listed below:

- 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:
- 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:

1. Adoption:

   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:

   Done by members and open for consultation from external parties.

- Interoperability level:
    - Organisational interoperability.
  - Standards:
    - Depends on specification.
  - Supporting organizations:
    - Not relevant.
  - Domain:
    - Multiple domains.
  - Application area:
    - Different specifications cover different areas. Smart City focus in some specifications.
  - Scope:
    - 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:
    - FRAND – ETSI IPR policy - http://www.etsi.org/about/how-we-work/intellectual-property-rights-iprs.
  - Specification Access:
    - 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:
    1. Adoption:

        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:

        Done by members and open for consultation from external parties.

- Interoperability level:
    - Organisational interoperability.
- Standards:
    - Depends on specification.
- Supporting organizations:
    - Not relevant.
- Domain:
    - Multiple domains.
- Application area:
    - Focus on access for all.
- Scope:
    - 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:
    - FRAND – ETSI IPR policy - http://www.etsi.org/about/how-we-work/intellectual-property-rights-iprs.
- Specification Access:
    - 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 ETSI TC ITS will be performed in close co-operation with relevant standards activities within and outside ETSI. The activities of ETSI TC ITS are:

- 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

ETSI TC ITS:

- Shall work in accordance with the normal rules as given in the ETSI Directives and, in particular, the Technical Working Procedures.
- Shall prepare ETSI deliverables of the type of EG, TR, TS, ES and EN.
- Shall provide progress reports to the ETSI Board and OCG from time to time.
- 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.
- 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 the 'verticals' is 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:

1. Adoption:

   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:

   Done by members and open for consultation from external parties.

- Interoperability level:
  - Organisational interoperability.
- Standards:
  - Depends on specification.
- Supporting organizations
  - ECC, CENELEC
- Domain:
  - Multiple domains.
- Application area:
  - Different specifications cover different areas. Smart City focus in some specifications.
- Scope:
  - 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:
  - FRAND – ETSI IPR policy - http://www.etsi.org/about/how-we-work/intellectual-property-rights-iprs.

- Specification Access:
    - Specification open ETSI web site – free to access for all.

ETSI TC MTS TST WG (Methods for Testing and Specification Testing WG)

- Description:

  Responsibility:
  The Testing WG („TST") develops studies, guidelines, test catalogues and test specifications for specific ICT technologies that are not already covered by existing ETSI Technical Bodies.

  The WG will strongly make use of the well-established test development languages and methodologies developed inside and outside TC MTS as appropriate.

  Within the ETSI TC MTS, experts from industry and research in multiple domains are working together on the application of advanced testing methods and techniques.

  Due to the speed of new development and the public demand to provide a common approach for reliable quality criteria a working group within TC MTS is a fast and appropriate means to provide international reference documents for industrial quality test criteria. A common approach for the test specification of IoT test purposes will support the interoperability, quality and confidence into the IoT industry.

  Organisation and working method

  Following the advanced test methodology developed within MTS it has been discussed and decided to apply TDL-TO for the definition of test purposes. This new ETSI notation is part of the overall approach for test developments in the ICT domain. From our technical work in the past, we know that it is essential to define test scenarios in a formal way to avoid misinterpretation and to allow the application of utilities supporting e.g. formatting or maintenance.

- Readiness:
    - Adoption

      Reference implementations
    - Development Status

      The technical specifications from TC MTS WG TST working programme have been finished and confirmed by ETSI TC MTS. The documents are available for the public from May 2021.
    - Openness

      Open to public
    - Ratification process

      Done by members and open for consultation from external parties
- Interoperability level:
    - Technical interoperability: addresses various IoT protocols and platforms (e.g. CoAP, MQTT, OPC-UA, LwM2M).
    - Syntactical interoperability: may be subject of future test catalogues
- Standards:
  Various SDO and consortia standards and protocols related to the protocols will be used and supported; sources will include IETF (CoAP), OASIS (MQTT), LoRa Alliance (LoRaWAN), IEC, etc.
- Supporting organizations:
    - Fraunhofer FOKUS
    - DEKRA Exam
    - Ericsson
    - AUDI

- Iskratel
- Spirent Communication
- Sintesio Foundation
- EasyGlobalMarket (EGM)

- Domain:
  - Initiative is related to multiple market domains (consumer/industrial internet) and the technical domain (connectivity, service and applications).
- Application area:
  - WG focus on horizontal industry, and do not exclude a particular vertical industry. Test types include, but are not limited to, conformance, security and performance.
- IPR Policy Available:

FRAND –http://www.etsi.org/about/how-we-work/intellectual-property-rights-iprs
Specification Access

- Published documents: https://www.etsi.org/standards/get-standards#page=1&search=&TB=860
- Work Item List: https://portal.etsi.org/tb.aspx?tbid=860&SubTB=860

ETSI TC Smart BAN (Smart Body Area Networks)

- Description:

ETSI TC SmartBAN is a vertical technical committee and shall have primarily responsibilities for development and maintenance of ETSI Standards, Specifications, Reports, Guides and other deliverables to support the development and implementation of Smart Body Area Network technologies (Wireless BAN, Personal BAN, Personal Networks etc.) in health, wellness, leisure, sport and other relevant domains

ETSI TC SmartBAN's scope includes communication media, and associated physical layer, network layer, security, QoS and lawful intercept, and also provision of generic applications and services (e.g. web) for standardisation in the area of Body Network Area technologies. Our target is to use what exists, fill in the gaps and make it work better and to help extend from today's fragmented BAN environment towards a harmonized SmartBAN.

Areas of activity

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

- Standardisation activities in all relevant areas to and preparation of ETSI: deliverables for the wireless Body Area Network for personal welfare.
- Close liaison with ETSI TC ERM, TC M2M, 3GPP and other relevant ETSI TBs.
- Co-ordination of Health ICT related requirements in order to produce a consistent set of ETSI deliverables and to undertake measures to efficiently continue and stimulate further Health ICT related work within ETSI.
- Provision of mechanisms for the effective liaison between ETSI TBs and with relevant external organisations such as SDOs, professionals from the areas of BAN applications, end-user representatives, local, national and regional Government Authorities, the European Commission, EU projects and Emergency Authorities/Organisations.
- Organisation of regular meetings/workshops with appropriate wireless Body Area Network for personal welfare stakeholders.
- Establishment of external relationships (and joint working groups) where and when ever needed, including co-operation with CONTINUA Alliance, Bluetooth SIG, CEN, CENELEC, ISO, HL7, IHE etc. Formal relationships will be established using the normal processes via the ETSI Secretariat (Partnerships).

Organizational and working methods

- ETSI TC SmartBAN shall work in accordance with the normal rules as given in the ETSI Directives and, in particular, the Technical Working Procedures.
- Existing related work and subsequent updates should remain in the current Technical Bodies (i.e. such as ERM (e.g. TG30 - Wireless Medical Devices), 3GPP, M2M, SCP, EMTEL, OCG Security, HF, etc.) and be co-ordinated with TC Smart BAN where relevant. New standards should only be prepared within TC SmartBAN where no appropriate ETSI Technical Body exists.
- Existing related work items should remain in current Technical Bodies. Updates to existing ETSI standard deliverables should be done within the appropriate Technical Bodies and be co-ordinated with ETSI TC SmartBAN where relevant. New standards should only be prepared within ETSI TC SmartBAN where no appropriate ETSI Technical Body exists.
- Where appropriate, joint working groups with other Technical Bodies may be created to develop deliverables for submission to the lead body.
- It is expected that ETSI TC SmartBAN members attending international standardisation meetings and fora as delegates will handle any necessary informal liaison with those group.

ETSI TC SmartBAN involved multiple organizations working in the context of an ETSI TC to develop SmartBAN standards:

- Work Item DTR/SmartBAN-004 (TR), Service and application enablers, standardized interfaces, APIs and infrastructure for heterogeneity/interoperability management:
    - ETSI TR 103 327 stable draft released
    - ETSI TR 103 327 consolidated version is being prepared and will address:

        1) SoA;

        2) Service/application level standardized APIs for Smart BAN entities (e.g. hub, relays, sensors, actuators) generic interactions;

        3) IoT compatible and multi-agent based architecture for SmartBAN generic data access/sharing, distributed monitoring and control operations, and interoperability management.
- Work Item DTS/SmartBAN-005 (TS), Low Complexity Medium Access Control and Routing:
    - Work Item closed and published.
- Work Item DTS/SmartBAN-006 (TR), Measurements and Modelling of SmartBAN RF environment:
    - STF511 on SmartBAN Performance and Coexistence Verification (PCV) in progress.
- Work Item DTS/SmartBAN-007 (TS), Enhanced Ultra-Low Power PHY:
    - Work Item is finished and published.
- Work Item DTR/SmartBAN-008, SmartBAN System Description:
    - Stable draft.
- Work Item DTS/SmartBAN-009 (TS), Unified data representation formats, semantic and open data model:
    - ETSI TS 103 378 release 1 has been published (20 December 2015).
    - ETSI TS 103 378 release 2 (added scope) is being prepared and will address:

        1) Specification and the formalization of SmartBAN service data model and ontology;

        2) Semantic interoperability.

- Readiness:

  1. Adoption:
     - No implementations/Reference implementations (according to the particular technical specification/report).

  2. Development Status:
     - Under development/Approved with no planned revisions/Approved with planned revisions (according to the particular technical specification/report).

  3. Compliance:
     - Not managed/Having compliance testing process (according to the particular technical specification/report).

  4. Openness:
     - Open by formal membership.

  5. Ratification process:
     - Done by members and open for consultation from external parties.

- Interoperability level:
  - Syntactical interoperability/Technical interoperability/Semantic interoperability (according to the particular technical specification/report).
- Standards:
  - Depends on the specification and the application.
- Supporting organizations:
  - Toshiba, CSEM, Oulu, Telecom SudParis, Florence, the Hermes Partrnership
- Domain:
  - Body Area Networks (BANs), from physical and Mac layer up to service and application level.
- Application area:
  - Relevant application areas include e.g. health, wellness, sports, medical, as well as retail sales, safety and other relevant domains for BAN. SmartBAN takes a system perspective.
- Scope:
  - Communication and Connectivity knowledge area:
    - ETSI TC SmartBAN's scope includes communication media, and associated physical layer, network layer, security, QoS and lawful intercept, and laso provision of generic applications and services (e.g. web) for standardization of BAN technologies.
  - Integration/Interoperability knowledge area:
    - SmartBAN covers specification of common IoT features required to provide integration and interoperability e.g. semantic interoperability for BAN in the IoT.
  - Applications knowledge area:
    - Communications and networks, hardware and software as well as service/application level enablers (e.g. semantic query, inference, rule management, discovery, monitoring and control …), applications.
  - Infrastructure knowledge area:
    - Communications and network connectivity.
  - IoT Architecture knowledge area:
    - covers integrated/complete IoT specification solutions, including architecture descriptions.

- Devices and sensor technology knowledge area:
    - Body sensor devices and other BAN equipped with SmartBAN technology inside (sensors, bracelets, watches, handsets, textiles, etc…).
- Security and Privacy knowledge area:
    - covers the relevant security, privacy trust issues for BAN (e.g. within the SmartBAN coordinator).

- IPR Policy Available:
    - ETSI standard IPR policy.
- Specification Access:
    - Specification open ETSI web site – free access for all.

ETSI TC Smart M2M

- Description:

Responsibility:

ETSI 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. Furthermore, ETSI TC Smart will support European policy and regulatory requirements including mandates in the area of M2M and the Internet of Things. The ETSI 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 ETSI TC Smart M2M.

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

- Readiness:

1. Adoption:

    Widely adopted in industry.

2. Development Status:

    Depends on specification, some published others under development.

3. Compliance:
4. Openness:

    Open to public – most groups some only open to members.

5. Ratification process:

    Done by members and open for consultation from external parties.

- Interoperability level:
    - Organisational interoperability.
- Standards:
    - Depends on specification.

- Supporting organizations:
  - Work in close cooperation with the OneM2M partnership project.
- Domain:
  - Multiple domains.
- Application area:
  - Different specifications cover different areas. Smart City focus in some specifications.
- IPR Policy Available:
  - FRAND – ETSI IPR Policy - http://www.etsi.org/about/how-we-work/intellectual-property-rights-iprs.
- Specification Access:
  - Specification open ETSI web site – free to access for all.

ETSI ISG CIM (Context Information Management)

- Description

  The goal of ETSI ISG CIM is to develop technical specifications and reports to enable multiple organisations to develop interoperable software implementations of a cross-cutting Context Information Management (CIM) Layer. It is about bridging the gap between abstract standards and concrete implementations. The ISG CIM Layer enables applications to update, manage, and access context information from many different sources, as well as publishing that information through interoperable data publication platforms.

- Readiness

  1. Adoption (users base): not new specification yet but a related API (called NGSI) is in widespread use in many FIWARE projects.

     Several implementation of the API are available, such as:

     - Orion-LD
     - Stellio Context broker
     - Scorpio broker
     - Developers Catalogue - FIWARE

  2. Development Status is "under development", first release due in Q3 2017
     - Specification and reports (GS and GR) under development
  3. Compliance will not be managed, however it is hoped to encourage open-source interoperability events.
  4. Openness is excellent, for any "legal entity" which signs ETSI IPR policy i.e. not only ETSI members but also research institutes and fora.
     - Open to public.
  5. Ratification of specifications is done by members and participants; the ISG is proactive for consultation with external parties.
     - Done by members and open for consultation from external parties

- Interoperability level
  - The specifications aim at organisational interoperability, which includes Semantic, Technical, and Syntactical interoperability.

- Standards:
    - After considering the use cases and a gap analysis with respect to existing protocols, the ISG CIM will consider in what way existing standardised protocols need to be modified to be fit-for-purpose for flexible context information management. Additionally, a large number of SDO specifications and documents are being examined from many related fields in information management.
    - Depends on specification.
- Supporting organizations (mainly for Alliances/OSS)
    - Not relevant
- Domain
    - The operating domain of the specifications is in the consumer area, facilitating mass-market and eGovernment enhancement of data with metadata (context). Industrial IoT will be considered at the end of the standardization process, to check if additional changes in the protocol might make it fit-for-purpose in some Smart Factory application areas.

        8. There is also being applied over different domains under the initiative called Smart Data Models (https://www.fiware.org/developers/smart-data-models/) in which there are exposed the common data models to be included in context broker to represent IoT information. In the case of the water domain, these data models are being developed through an initiative of several EU funded projects.
- Application area
    - The work of ISG CIM is absolutely devoted to horizontal frameworks, for all kinds of vertical IoT domains, however, to keep the work practical the initial use cases are considered for the SmartCity, vertical (expanding later to SmartAgriculture, Smart Water, SmartFactory, etc.).
- IPR Policy Available
    - ETSI IPR Policy (FRAND) is followed as set forth in Annex 6 of the ETSI Rules of Procedure, see http://www.etsi.org/about/how-we-work/intellectual-property-rights-iprs. Note that the ToR of ETSI ISG CIM expresses desire for 'collaboration with open source initiatives supporting the specifications'.
- Specification Access
    - Approved specifications will be published on the ETSI website, as for all TR and TS documents. Additionally, the ISG CIM has a policy to solicit public comment on draft specifications and has create an open area for publishing (after obtaining ETSI administrative support) specific documents: https://docbox.etsi.org/ISG/CIM/Open

ETSI ISG MEC (Multi-access-Edge Computing)

- Description:
  Mobile-access 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), MEC 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.
- Supports 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:
  1. Adoption:

     Yes, several implementations are available; Open-source repository for APIs: https://forge.etsi.org/rep/mec

  2. Development Status:

     - Specification under development. (upgrades, corrections, inputs from other organisations).

  3. Compliance:

     - Robot test suite: https://hub.docker.com/r/etsiforge/mec-robot-hivetap-tt

  4. Openness:

     Open to public.

  5. Ratification process:

     Done by members and open for consultation from external parties.

- Interoperability level:
  - Organisational interoperability.
- Standards:
  - Latest APIs from the Multi-access Edge Computing ISG:
    - Application package lifecycle and operation granting API - GS 010-2
    - Multi-access Edge Platform Application Enablement API - GS 011
    - Radio Network Information API - GS 012
    - Location API - GS 013
    - UE Identity API - GS 014
    - Bandwidth Management API - GS 015
    - UE Application Interface API - GS 016
    - Application Mobility Service API – GS 021
    - MEC WLAN Information API - GS 028
    - Fixed Access Information API - GS 029
    - V2X Information Service API – GS 030
  - Abstract Test Suites from the Multi-access Edge Computing ISG at:
    - TTCN-3 Test Suite - GS 032 API Conformance Specification, Part 3
    - Robot Framework Test Suite - GS 032 API Conformance Specification, Part 3
- Supporting organizations:
  - Membership list: https://portal.etsi.org/TB-SiteMap/MEC/List-of-Members
- Domain:
  - Multiple domains.
- Application area:
  - Different specifications cover different areas. Smart City focuses in some specifications.
  - PoCs available: https://www.etsi.org/technologies/multi-access-edge-computing/mec-poc
- IPR Policy Available:
  - FRAND – ETSI IPR policy - http://www.etsi.org/about/how-we-work/intellectual-property-rights-iprs.
- Specification Access:
  - Specifications are open via the ETSI website – free to access for all.

ETSI ISG NFV (Network Functions Virtualisation)

- Description:

  The purpose of ISG NFV is to facilitate the industry transformation and the development of an open, interoperable, ecosystem enabling managing the lifecycle of virtualised network functions hosted on independently deployed and operated NFV infrastructure platforms, which can be distributed across various locations (e.g. centralised data centres, edge clouds, end user premises, etc.).

  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 focused on producing the technical specifications for the NFV foundation technology. During the 2017-2020 period, the ISG focused on consolidating these technical specifications, defining a consistent operational integration with current network services, and addressing the additional requirements for NFV technologies brought by the evolution of telecommunications networks, especially in what relates to 5G, in close cooperation with global and regional initiatives.

  From 2021 onwards, ISG NFV will continue to further consolidate technical specifications and address new functional and operational requirements brought by new use cases (e.g. for industry verticals) and operational models, leveraging advances in network management, orchestration, virtualisation and Cloud technologies.

  The ISG NFV will address technical challenges that include:

  - Ensuring that virtualised network platforms will be able to support automated (and even autonomous) management of all application-independent aspects of virtualised services, ranging from the management of the virtualised resources they use to the management of the network functions they combine.
  - Achieving high-performance virtualised network functions which are portable between different supporting platforms, which includes hardware, infrastructure software, and orchestration stacks.
  - Achieving co-existence with legacy hardware-based network platforms whilst enabling an efficient migration path to fully virtualised network platforms.
  - Catalysing the evolution of network management support systems to take full advantage of virtualisation and software-based operation techniques.
  - Ensuring the security of virtualised network platform from attack and misconfiguration, and their compliance with national and international regulations on privacy and security matters.
  - Maintaining network stability and service levels without degradation during any event in the functions lifecycle.
  - Ensuring the appropriate level of resilience to hardware and software failures, operational errors, and other anomalous events.
  - Exploring the necessary enabling technologies to support the new business models made possible by network virtualisation.
  - Exploring technologies enabling cross-organizational continuous integration and continuous delivery practices in software-based virtualised environments.

9. The activities of ISG NFV include the following broad areas:
   - Resource virtualization (storage, compute, network),
   - Network Slicing,
   - Hardware and software acceleration,
   - Management and orchestration (of Virtualised Network Functions, of infrastructure resources, etc.),
   - Performance, Reliability, Resiliency,

- Architecture (component and interface definition),
- Information and data modelling,
- Protocols, Application Programming Interface,
- Security, trust, attestation, regulation,
- Testing, benchmarking, continuous integration and development processes
- Readiness:

  1. Adoption:
     - Widely adopted in industry.

  2. Development Status:
     - ISG NFV has developed over 100 different specifications and reports for the virtualization of network functions, with focus on the management and orchestration of virtualized resources.
     - ISG NFV works on a number of Releases in parallel. The development status of the specifications depends on the Release they belong to.
       - Under development: Release 4, Release 5
       - Approved with no planned revisions: Release 1, Release 2
       - Approved with planned revisions: Release 3

  3. Compliance:
     - Having compliance testing process (include test suites, method, etc.)
       - Conformance test suites for Management and Orchestration APIs, including robot code:
         - https://forge.etsi.org/rep/nfv/api-tests
       - Conformance and Interoperability tests held regularly at ETSI Plugtests™ events.
         - https://www.etsi.org/technologies/nfv/nfv-plugtests-programme

  4. Openness:
     - Results and work programme are public.
     - Participation is open to ETSI members as well as non-members having signed the participation agreement.

  5. Ratification process:
     - Done by members and open for consultation from external parties

- Interoperability level:
  - ISG NFV develops and maintains a full set of standards enabling an open ecosystem where Virtualized Network Functions (VNFs) can be interoperable with independently developed management and orchestration systems, and where the components of a management and orchestration system are themselves interoperable.
    - Syntactical interoperability.
    - Technical interoperability.
    - Semantic interoperability.
    - Organizational interoperability
- Standards:
  - ISG NFV has developed over 100 different specifications and reports for the virtualization of network functions, with focus on the management and orchestration of virtualized resources. This includes a set of Restful API specifications, the specifications of a packaging format for delivering VNFs to service providers, as well as TOSCA-based and YANG-based specification of the deployment templates packaged with the VNF software images to enable managing the lifecycle of VNFs.

        - The latest publications can be found here: https://www.etsi.org/committee/1427-nfv
        - and the associated code, here: https://forge.etsi.org/rep/nfv
    - Supporting organizations
        - 125 member or participant organizations from both the Telco and IT industry.
        - Participation from academia is encouraged through the publication of a Research Agenda
            - https://docbox.etsi.org/ISG/NFV/Open/Other/NFV_Research_Agenda-202104.pdf
        - List of member and participant organizations : https://portal.etsi.org/TB-SiteMap/NFV/NFV-List-members
    - Domain:
        - Multiple domains on both axis.
    - Application area:
        - ISG NFV develops a generic framework applicable to any kind of network function. ETSI GS NFV 001 describes typical use cases, including an IoT use case.
            - https://www.etsi.org/deliver/etsi_gr/NFV/001_099/001/01.03.01_60/gr_nfv001v010301p.pdf
    - IPR Policy Available:
        - FRAND – ETSI IPR policy - http://www.etsi.org/about/how-we-work/intellectual-property-rights-iprs.
    - Specification Access:
        - Find publicly available NFV specifications via the NFV committee page, and subscribe for alerts on updates of specifications (free to access for all).
            - https://www.etsi.org/committee/1427-nfv
        - The associated code can be found here
            - https://forge.etsi.org/rep/nfv
        - In addition to the published specifications, ISG NFV makes all of its drafts in progress publicly available for industry comment.
            - http://docbox.etsi.org/ISG/NFV/Open/Drafts/

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:

  1. Adoption:
     - 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:

     Done by members and open for consultation from external parties.

- Interoperability level:
  - Organisational interoperability.
- Standards:
  - Depends on specification.
- Supporting organizations:
  - Not relevant.
- Domain:
  - Multiple domains.
- Application area:
  - Energy efficiency.
- Scope:
  - Infrastructure knowledge area.
- IPR Policy Available:
  - FRAND – ETSI IPR policy - http://www.etsi.org/about/how-we-work/intellectual-property-rights-iprs.
- Specification Access:
  - Specification open ETSI web site – free to access for all.

5.2.7 Fairhair

- Description:
  - Fairhair is an Alliance of leading companies, from the Lighting, Building Automation and IT industry, that aims to facilitate the 'Internet of Things' for buildings. The vision of the Fairhair Alliance is that of a cost effective, certified and secure IP-based, common network infrastructure that can serve as a basis for interoperable Lighting and Building Automation systems. This will enable a move from proprietary, standalone solutions to a common building network infrastructure that supports the 'IoT' of resource constrained devices, including sensors, lamps, luminaries, thermostats, dimmers and so on.
- Readiness:
  1. Adoption:
     - No implementations.
  2. Development Status:
     - Under development.
  3. Compliance:
     - Yes, described in bylaws.
  4. Openness:
     - Open by formal membership.
  5. Ratification process:
     - By general assembly in accordance to voting rules.
- Interoperability level:
  - Technical, syntactical, semantic.
- Standards:
  - The Fairhair Alliance will collect the requirements of the Lighting and Building Automation industries and use this information to develop a set of technical specifications for a common IP-based infrastructure, based on open IEEE and IETF standards. The Alliance will liaise with the relevant eco-systems to promote and support adoption of the Fairhair specifications.
- Supporting organizations:
  - http://www.fairhair-alliance.org/about-fairhair/membership.html.
- Domain:
  - Service & applications from B2C to B2B.
- Application area:
  - Smart Building (Building Automation and Lighting).
- Scope:
  - Communication and Connectivity.
  - Integration/Interoperability.
  - Applications.
- IPR Policy Available:
  - RAND RF License.
- Specification Access:
  - Only for regular or sponsor members.

5.2.8 GlobalPlatform

- Description:
  - GlobalPlatform is a non-profit, member driven association which defines and develops specifications to facilitate the secure deployment and management of multiple applications on secure chip technology. Its standardized infrastructure empowers service providers to develop digital services once and deploy them across different devices and channels. GlobalPlatform's security and privacy parameters enable dynamic combinations of secure and non-secure services from multiple providers on the same device, providing a foundation for market convergence and innovative new cross-sector partnerships.
  - GlobalPlatform is the international industry standard for trusted end-to-end secure deployment and management solutions. The technology's widespread global adoption across finance, mobile/telecom, government, premium content, automotive, healthcare, retail and transit sectors delivers cost and time-to-market efficiencies to all. GlobalPlatform supports the long-term interoperability and scalability of application deployment and management through its secure chip technology open compliance program.
  - With cross market representation from all continents, GlobalPlatform's 120+ members contribute to its technical committees and market-led task forces, ensuring full alignment with existing and emerging market requirements.
  - Details on GlobalPlatform can be found via: http://www.globalplatform.org/aboutus.asp.
- Readiness:

1. Adoption:

   Widely adopted in industry.

2. Development Status:

   Approved with planned revisions.

3. Compliance:

   Formal certification process.

4. Openness:

   Open by formal membership then public when finalized.

5. Ratification process:

   Done by members and open for consultation from external parties.

- Interoperability level:
  - Syntactical interoperability
  - Technical interoperability
  - Semantic interoperability
  - Organisational interoperability
- Standards:
  - Depends on specification
- Supporting organizations:
  - See http://www.globalplatform.org/aboutusindustryrel.asp

- Domain:
    - GlobalPlatform provides specifications to provide secure services by allowing the deployment and the management of specific application from a service provider. Many global industries, including payments, transportation, healthcare, government, enterprise ID / authentication and premium content can use the GP technology to build their service. GlobalPlatform defines two secure component options: a Secure Element (SE) and a Trusted Execution Environment (TEE). When a service provider deploys their service into a secure component within a device, they benefit from a trusted 'anchor' within that device. This allows them to manage risk associated with their service effectively and confidently.
- Application area:
    - The Application area is wide as the secure component (either the SE or the TEE) can be used in a lot of different form factors. The most well-know, but not limitative are the mobile, the UICC, the smartcard.
- Scope:
    - 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:
    - FRAND or RAND, see http://www.globalplatform.org/membershipipr.asp
- Specification Access:
    - Public specifications are free
    - Configurations are free for members and available at a fee for non-members.
    - Draft specifications are accessible by members only

5.2.9 GS1

- Description:

  GS1 is an international federation of not-for-profit organisations established in 112 countries with a total of more than one million member companies. GS1 manages a global identification system for items, parties, locations, assets, etc., a comprehensive set of automatic data capture standards using barcodes and RFID as well as standards for the electronic sharing of information.

  The large majority of GS1 standards fall under the IoT flag. The Auto-ID Center initiative at MIT in the early two thousands developed the EPC and other technical concepts and standards prevalent today in the global RFID industry. It coined the term Internet of Things which envisioned objects /things connected to object-specific data on the internet which could be accessed using the unique EPC on the tag attached to the object. As of 2003, GS1 took over the concept through its fully owned EPCglobal subsidiary. Formal standards were developed and the technology was brought to the market for implementation. EPCIS that is also published as ISO/IEC 19987 is a GS1 standard that defines a common data model for visibility data and interfaces for capturing and sharing visibility data within an enterprise and across an open supply chain.

- Readiness:

  1. Adoption:
     - Widely adopted in industry.
  2. Development Status:
     - Approved with planned revisions.
  3. Compliance:
     - Having compliance testing process.
  4. Openness:
     - Open by formal membership.
  5. Ratification process:
     - Done primarily by members but external parties may submit comments.

- Interoperability level:
  - The GS1 system architecture promotes interoperability. GS1 system components and any underlying processes that are developed strive to be interoperable in their design, development, and implementation to enable the widest adoption and usage by the User community. All GS1 standards are compliant with widely accepted technical standards from internationally recognised SDOs such as ISO, W3C, IETF and UN/CEFACT:
    - Syntactical interoperability.
    - Technical interoperability.
    - Semantic interoperability.
    - Organisational interoperability.

- Standards:
  - All GS1 standards are compliant with widely accepted technical standards from internationally recognised SDOs such as ISO, W3C, UN/CEFACT and IETF.

- Supporting organizations:
  - Large and small companies from various sectors including consumer goods, retail, healthcare, transport & logistics as well as solution providers. This broad support is well reflected in the diversity of the GS1 Management Board members, http://www.gs1.org/about/management-board.

- Domain:
  - The main scope of application of GS1 standards is in B2B processes. There are however more and requirements and therefore GS1 standards and services addressing the B2C area. GS1 focuses on services and applications rather than technical connectivity. It should thus be positioned in the upper right quadrant of the landscape.

- Application area:
    - The application area is mainly business to business supply chain processes. The main industry sectors using the GS1 system of standards are retail, healthcare and transport / logistics. There are however implementations in many other sectors.
- Scope:
    - 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: Royalty fee or RAND, see http://www.gs1.org/ip.
- Specification Access: All specifications are available publicly and free of charge, see http://www.gs1.org/standards.

5.2.10 GSMA (GSM Association)

- Description:
  - 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:

1. Adoption:
   - Widely adopted in industry.
2. Development Status:
   - Approved with planned revisions.
3. Compliance:
   - Not managed.
4. Openness:
   - Open by formal membership.
5. Ratification process:
   - Closed process done by members only with no consultation from external parties.

- Interoperability level:
  - Technical interoperability.
- Standards:
  - 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
  - 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:
  - GSMA make just one standard, eSIM. It locates in the connectivity domain, and can be used for both consumer and industrial market.
- Application area:
  - 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.
- IPR Policy Available:

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

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

5.2.11 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.

5.2.12 IEC (International Electrotechnical Commission)

This section provides a brief description of the International Electrotechnical Commission (IEC) 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, such as: 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).

Moreover, the 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, tele-protection, 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:
  1. Adoption:
     - Widely adopted in industry.
  2. Compliance:
     - Not managed by IEC.
  3. Openness:
     - Open to public.
  4. Ratification process:
     - Done by members and open for consultation from external parties.

- Interoperability level:
    1. Syntactical interoperability.
    2. Technical interoperability.
    3. Semantic interoperability.
- Standards:
    - 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:
    - Energy, Smart Grid, Smart Cities.
- Domain:
    - Industrial.
- Application area:
    - Smart Grid, Smart City.
- IPR Policy Available:
    - ITU / ISO / IEC code of practice.
    - FRAND.
- Specification Access:
    - 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:

- Device integration with industrial automation systems. The models developed in these standards address device properties, classification, selection, configuration, commissioning, monitoring and basic diagnostics.
- Industrial automation systems integration with enterprise systems. This includes transactions between business and manufacturing activities which may be jointly developed with ISO TC184.

- Readiness:

1. Adoption:
    - Widely adopted in industry.
2. Compliance:
    - Not managed by IEC.
3. Openness:
    - Open to public.
4. Ratification process:
    - Done by members and open for consultation from external parties.
        - Interoperability level:

- Syntactical interoperability.
- Technical interoperability.
- Semantic interoperability.
- Organisational interoperability.

- Standards:

Publication Examples:

- 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:
    - Manufacturing.
    - Industrial automation.
- Domain:
    - Industrial.
- Application area:
    - Smart manufacturing.
- IPR Policy Available:
    - ITU / ISO / IEC code of practice.
    - FRAND.
- Specification Access:
    - Open to everyone with a fee.

5.2.13 IEEE Standards Association

- Description:

  IEEE Standards Association mission is for advancing technology for the benefit of humanity by providing a globally open, inclusive and transparent environment for market relevant, voluntary consensus standardization. The objective of IOT Standardization is to establish reference framework and architecture for Internet of Things. The architectural framework defined in the IEEE 2413 standard will promote cross-domain interaction, aid system interoperability and functional compatibility across IOT systems. IEEE-SA also develops several other IOT standards across different verticals – Communications (IEEE 802 – wireless/wireline standards, IEEE 1901 on BPL), Transportation (IEEE 802.11p, IEEE 1609P), eHealth (11073), Smart Grid standards and Smart Energy Profile (IEEE 2030.5), and Sensor Standards (IEEE 1451, IEEE 2700) to name a few of the IEEE standards.

- Interoperability level:
  - The various standards of the IEEE Standards Association address all the different levels of interoperability as mentioned below:
    - Syntactical interoperability.
    - Technical interoperability.
    - Semantic interoperability.
    - Organizational interoperability.
- Standards:
  - The standards activities of IEEE on IoT are numerous as is indicated on the IEEE Internet of Things initiative web site -http://standards.ieee.org/innovate/iot/stds.html.
- Supporting organizations:
- Domain:
  - Health
  - Smart City
- Application area:
- IPR Policy Available:
  - The IEEE-SA Patent Policy is section 6 of the IEEE-SA Standards Board Bylaws (http://standards.ieee.org/develop/policies/bylaws/sect6-7.html). See also http://standards.ieee.org/about/sasb/patcom/materials.html.
- Availability:
  - IEEE-SA standards are available openly for the public. They can be obtained from IEEE (http://ieeexplore.ieee.org/Xplore/guesthome.jsp or http://www.techstreet.com/ieee). The IEEE-SA policies can be viewed at https://standards.ieee.org/develop/policies/

5.2.14 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:
  1. Adoption:
     - Reference implementations
  2. Development Status:
     - Under development.
  3. Compliance:
     - Not managed.
  4. Openness:
     - Open by formal membership.
  5. Ratification process:
     - Done by members and open for consultation from external parties.
- Standards:
  - P2413 Standard for an Architectural Framework for the Internet of Things.
- Supporting organizations
  - Not relevant.
- Domain:
  - Market: consumer and industrial.
  - Technology: closer to service & applications.
- Application area:
  - Horizontal.
- Scope:
  - IoT Architecture knowledge area.
- IPR Policy Available:
  - FRAND, royalty free.
- Specification Access:
  - Open to everyone with a fee.

5.2.15 IEEE P2874 SPATIAL WEB Protocol, Architecture and Governance Working Group

- Description:

  IEEE P2874 Standard for Spatial Web Protocol, Architecture and Governance Working Group.

  This standard describes a Hyperspace Transaction Protocol (HSTP) that enables interoperable, semantically compatible connections between connected hardware (e.g. autonomous drones, sensors, smart devices, robots) and software (e.g. services, platforms, applications, artificial intelligence systems) and includes specifications for:

  1. a spatial range query format and response language for requesting data about objects within a dimensional range (spatial, temperature, pressure, motion) and their content.
  2. a semantic data ontology schema for describing objects, relations, and actions in a standardized way
  3. a verifiable credentialing and certification method for permissioning create, retrieve, update, and delete (CRUD) access to devices, locations, users, and data; and
  4. a human and machine-readable contracting language that enables the expression and automated execution of legal, financial and physical activities.

- Readiness:

  1. Adoption:
     - Reference implementations
  2. Development Status:
     - Under development.
  3. Compliance:
  4. Openness:
     - Open to public, based on IEEE rules
  5. Ratification process:
     - Following IEEE process, i.e., done by members and open for consultation from external parties.

- Standards:
  - This is a new standard that may include references to existing standards and specifications such as TCP/IP, http, html, W3C DID's and Verifiable Credentials.
- Supporting organizations
  - IEEE and Spatial Web Foundation (SWF), see: https://spatialwebfoundation.org/
- Domain:
  - The Standards are related to multiple market domains (consumer/industrial internet) and the technical domain (connectivity, service and applications).
- Application area:
  - WG focus on, i.e. horizontal industry, and do not exclude a particular vertical industry. Test types include, but are not limited to, conformance, security and performance.
- Scope:
  - IEEE P2874 Standard for Spatial Web Protocol, Architecture and Governance Working Group.
- IPR Policy Available:
  - IEEE copyright policy https://www.ieee.org/publications/rights/copyright-policy.html
- Specification Access:
  - https://sagroups.ieee.org/2874/

5.2.16 IETF (Internet Engineering Task Force)

This section provides a brief description of the IETF (Internet Engineering Task Force) initiative and its edge computing 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:

- Reference implementations and interoperability plug test events done by ETSI.

2. Development Status:

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

3. Compliance:

- Not IETF responsibility.

4. Openness:

- Open to public.

5. Ratification process:

- Open process for all parties interested in the ratification.

- Interoperability level:
  - Syntactical interoperability.
  - Technical interoperability.
  - Semantic interoperability.
- Standards:

Document	Date	Status	
Active Internet-Drafts (7 hits)			
draft-ietf-6lo-ap-nd-12 Address Protected Neighbor Discovery for Low-power and Lossy Networks	2019-04-10 28 pages	AD Evaluation for 82 days Submitted to IESG for Publication: Proposed Standard	
draft-ietf-6lo-backbone-router-12 IPv6 Backbone Router	2019-09-02 30 pages	I-D Exists In WG Last Call	1
draft-ietf-6lo-deadline-time-05 Packet Delivery Deadline time in 6LoWPAN Routing Header	2019-07-08 21 pages	IESG Evaluation::AD Followup for 130 days Submitted to IESG for Publication: Proposed Standard Reviews: genart, intdir, iotdir, opsdir, rtgdir, secdir	
draft-ietf-6lo-fragment-recovery-05 6LoWPAN Selective Fragment Recovery	2019-07-22 26 pages	I-D Exists WG Document	
draft-ietf-6lo-minimal-fragment-04 6LoWPAN Fragment Forwarding	2019-09-02 8 pages	I-D Exists WG Document	
draft-ietf-6lo-nfc-15 Transmission of IPv6 Packets over Near Field Communication	2019-07-08 17 pages	IESG Evaluation::AD Followup for 193 days Submitted to IESG for Publication: Proposed Standard Reviews: genart, intdir, iotdir, opsdir, secdir, tsvart	1
draft-ietf-6lo-use-cases-07 IPv6 over Constrained Node Networks (6lo) Applicability & Use cases	2019-09-10 23 pages New	I-D Exists In WG Last Call	
RFC 7388 (was draft-ietf-6lo-lowpan-mib) Definition of Managed Objects for IPv6 over	2014-10 27 pages	Proposed Standard RFC	

Document	Date	Status
Low-Power Wireless Personal Area Networks (6LoWPANs)		
RFC 7400 (was draft-ietf-6lo-ghc) 6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)	2014-11 24 pages	Proposed Standard RFC
RFC 7428 (was draft-ietf-6lo-lowpanz) Transmission of IPv6 Packets over ITU-T G.9959 Networks	2015-02 21 pages	Proposed Standard RFC
RFC 7668 (was draft-ietf-6lo-btle) IPv6 over BLUETOOTH(R) Low Energy	2015-10 21 pages	Proposed Standard RFC
RFC 7973 (was draft-ietf-6lo-ethertype-request) Assignment of an Ethertype for IPv6 with Low-Power Wireless Personal Area Network (LoWPAN) Encapsulation	2016-11 5 pages	Informational RFC
RFC 8025 (was draft-ietf-6lo-paging-dispatch) IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Paging Dispatch	2016-11 8 pages	Proposed Standard RFC
RFC 8065 (was draft-ietf-6lo-privacy-considerations) Privacy Considerations for IPv6 Adaptation-Layer Mechanisms	2017-02 10 pages	Informational RFC
RFC 8066 (was draft-ietf-6lo-dispatch-iana-registry) IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) ESC Dispatch Code Points and Guidelines	2017-02 9 pages	Proposed Standard RFC
RFC 8105 (was draft-ietf-6lo-dect-ule) Transmission of IPv6 Packets over Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE)	2017-05 22 pages	Proposed Standard RFC
RFC 8505 (was draft-ietf-6lo-rfc6775-update) Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery	2018-11 47 pages	Proposed Standard RFC

- Supporting organizations
  - 6lo is an IETF WG.
- Domain:
  - 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 and applications edge of the vertical axis.
- Application area:
  - 6lo WG is focusing on horizontal industry.
- Scope:
  - 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:
  - 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.

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. The work items of this working group are:

- 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.
- 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.
- 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.

- Readiness:

1: Adoption:

- Reference implementations and interoperability plug test events done by ETSI.

2. Development Status:

Date	Milestone
Done	6TiSCH architecture and terminology in RFC publication queue
Dec 2018	Evaluate WG progress, propose new charter to the IESG
Done	Initial submission of 6TiSCH architecture to the IESG
Oct 2018	Initial submission of draft-ietf-6tisch-dtsecurity-zerotouch-join to the IESG
Done	Initial submission of draft-ietf-6tisch-minimal-security to the IESG
Done	Initial submission of draft-ietf-6tisch-6top-protocol to the IESG
Done	ETSI 6TiSCH #3 plugtests
Done	WG call to adopt draft-ietf-6tisch-6top-sublayer
Done	WG call to adopt draft-ietf-6tisch-6top-sf0
Done	Second submission of draft-ietf-6tisch-minimal to the IESG

3. Compliance:

- Not IETF responsibility.

4. Openness:

- Open to public.

5. Ratification process:

- Open process for all parties interested in the ratification.

- Interoperability level:
  - Syntactical interoperability.
  - Technical interoperability.
  - Semantic interoperability.
- Standards:

Document	Date	Status	
Active Internet-Drafts (5 hits)			
draft-ietf-6tisch-architecture-26 An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4	2019-08-27 70 pages	IESG Evaluation::AD Followup for 46 days Submitted to IESG for Publication: Informational Reviews: genart, intdir, iotdir, opsdir, rtgdir, secdir, tsvart	3
draft-ietf-6tisch-dtsecurity-zerotouch-join-04 6tisch Zero-Touch Secure Join protocol	2019-07-08 27 pages	I-D Exists WG Document	
draft-ietf-6tisch-enrollment-enhanced-beacon-05 IEEE802.15.4 Informational Element encapsulation of 6tisch Join and Enrollment Information	2019-09-16 8 pages New	Publication Requested for 6 days Submitted to IESG for Publication: Proposed Standard	
draft-ietf-6tisch-minimal-security-12 Minimal Security Framework for 6TiSCH	2019-07-29 50 pages	In Last Call (ends 2019-10-04) for 3 days Submitted to IESG for Publication: Proposed Standard	
draft-ietf-6tisch-msf-06 6TiSCH Minimal Scheduling Function (MSF)	2019-08-12 19 pages	I-D Exists WG Document	1
RFC 7554 (was draft-ietf-6tisch-tsch) Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the	2015-05 23 pages	Informational RFC	

Document	Date	Status
Internet of Things (IoT): Problem Statement		
RFC 8180 (was draft-ietf-6tisch-minimal) Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration	2017-05 28 pages	Best Current Practice RFC
RFC 8480 (was draft-ietf-6tisch-6top-protocol) 6TiSCH Operation Sublayer (6top) Protocol (6P)	2018-11 50 pages	Proposed Standard RFC

- Supporting organizations
  - 6TiSCH is an IETF WG.
- Domain:
  - 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 and applications edge of the vertical axis
- Application area:
  - 6TiSCH WG is focusing on horizontal industry.
- Scope:
  - 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:
  - 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:
    1. Adoption:
    2. Development Status:

Date	Milestone
Done	Submit ACE profile for OSCORE to the IESG for publication as a Proposed Standard
Nov 2018	Submit DTLS Profile for ACE to the IESG for publication as a proposed standard
Done	Submit "Authentication and Authorization Solution" specification to the IESG for publication as a Proposed Standard.
Done	WGLC on OSCORE Profile for ACE
Done	WGLC for DTLS Profile for ACE
Done	WGLC for OAuth Authentication and Authorization Solution draft
Done	Submit CWT Proof of Possession to IESG for publication as proposed standard
Done	WGLC on CWT Proof of possession
Done	Submit CBOR Web Token draft to the IESG for publication
Done	Submit "Authentication and Authorization for ACE" specification as a WG item.
Done	Optionally, submit "Use cases and Requirements" document to the IESG for publication as an Informational RFC.
Done	Submit "An Architecture for Authorization in Constrained Environments" as a WG item.
Done	Submit "Use cases and Requirements" as a WG item.

    3. Compliance:
        - Having compliance testing process (include test suites, method, etc.).
        - Formal certification process.
    4. Openness:
        - Open to public.
    5. Ratification process:
        - Done by members and open for consultation from external parties.
        - Open process for all parties interested in the ratification.
- Interoperability level:
    - Syntactical interoperability.
    - Technical interoperability.

- Standards:

Document	Date	Status
Active Internet-Drafts (9 hits)		
draft-ietf-ace-cwt-proof-of-possession-07 Proof-of-Possession Key Semantics for CBOR Web Tokens (CWTs)	2019-09-18 16 pages New	AD Evaluation::AD Followup for 49 days Submitted to IESG for Publication: Proposed Standard
draft-ietf-ace-dtls-authorize-08 Datagram Transport Layer Security (DTLS) Profile for Authentication and Authorization for Constrained Environments (ACE)	2019-04-12 21 pages	Publication Requested for 139 days[1] Submitted to IESG for Publication: Proposed Standard
draft-ietf-ace-key-groupcomm-02 Key Provisioning for Group Communication using ACE	2019-07-05 36 pages	I-D Exists WG Document
draft-ietf-ace-key-groupcomm-oscore-02 Key Management for OSCORE Groups in ACE	2019-07-05 30 pages	I-D Exists WG Document
draft-ietf-ace-mqtt-tls-profile-00 MQTT-TLS profile of ACE	2019-05-08 22 pages	I-D Exists WG Document
draft-ietf-ace-oauth-authz-24 Authentication and Authorization for Constrained Environments (ACE) using the OAuth 2.0 Framework (ACE-OAuth)	2019-03-27 83 pages	AD Evaluation for 56 days[1] Submitted to IESG for Publication: Proposed Standard
draft-ietf-ace-oauth-params-05 Additional OAuth Parameters for Authorization in Constrained Environments (ACE)	2019-03-25 13 pages	Publication Requested for 202 days Submitted to IESG for Publication: Proposed Standard
draft-ietf-ace-oscore-profile-08 OSCORE profile of the Authentication and Authorization for Constrained Environments Framework	2019-07-08 27 pages	Publication Requested for 202 days Submitted to IESG for Publication: Proposed Standard
RFC 7744 (was draft-ietf-ace-usecases) Use Cases for Authentication and Authorization in Constrained Environments	2016-01 30 pages	Informational RFC
RFC 8392 (was draft-ietf-ace-cbor-web-token) CBOR Web Token (CWT)	2018-05 25 pages	Proposed Standard RFC

- Supporting organizations
  - ACE is an IETF WG.
- Domain:
  - 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 and applications edge of the vertical axis.
- Application area:
  - ACE WG is focusing on horizontal industry.
- Scope:
  - 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:
  - 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

    10. 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:

    - Reference implementations.
    - Widely adopted in industry.

    2. Development Status:

    - Approved with planned revisions.

Date	Milestone
Dec 2099	CoRE Interfaces submitted to IESG
Mar 2018	CoRE Resource Directory submitted to IESG for PS
Jan 2018	Management over CoAP submitted to IESG for PS
Dec 2017	Object Security for Constrained RESTful Environments (OSCORE)
Dec 2017	CBOR Encoding of Data Modeled with YANG submitted to IESG for PS
Dec 2017	Media Types for Sensor Measurement Lists (SenML) submitted to IESG for PS
Done	CoAP over TCP, TLS, and WebSockets submitted to IESG for PS
Done	WG adoption for Management over CoAP
Done	Patch and Fetch Methods for CoAP submitted to IESG for PS
Done	Representing CoRE Link Collections in JSON submitted to IESG
Done	Best Practices for HTTP-CoAP Mapping Implementation submitted to IESG
Done	Blockwise transfers in CoAP submitted to IESG

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

- Interoperability level:
    - Syntactical interoperability.
    - Technical interoperability.
    - Semantic interoperability.
- Standards:
    - The IETF CORE WG is specifying the COAP protocol.

Document	Date	Status	
Active Internet-Drafts (16 hits)			
draft-ietf-core-comi-07 CoAP Management Interface	2019-07-22 50 pages	I-D WG Document	Exists
draft-ietf-core-coral-00 The Constrained RESTful Application Language (CoRAL)	2019-08-29 42 pages	I-D WG Document	Exists
draft-ietf-core-dynlink-10 Dynamic Resource Linking for Constrained RESTful Environments	2019-07-22 24 pages	I-D WG Document	Exists
draft-ietf-core-echo-request-tag-07 CoAP: Echo, Request-Tag, and Token Processing	2019-09-19 27 pages New	I-D In WG Last Call	Exists
draft-ietf-core-hop-limit-05 Constrained Application Protocol (CoAP) Hop-Limit Option	2019-09-10 8 pages New	In Last Call (ends 2019-09-27) for 10 days Submitted to IESG for Publication: Proposed Standard Reviews: genart, opsdir, secdir	
draft-ietf-core-href-00 Constrained Resource Identifiers	2019-08-29 15 pages	I-D WG Document	Exists
draft-ietf-core-multipart-ct-04 Multipart Content-Format for CoAP	2019-08-21 10 pages	IESG Evaluation::AD Followup for 144 days Submitted to IESG for Publication: Proposed Standard Reviews: genart, opsdir, secdir	
draft-ietf-core-oscore-groupcomm-05 Group OSCORE - Secure Group Communication for CoAP	2019-07-05 49 pages	I-D WG Document	Exists
draft-ietf-core-rd-dns-sd-05 CoRE Resource Directory: DNS-SD mapping	2019-07-07 14 pages	I-D WG Document	Exists
draft-ietf-core-resource-directory-23 CoRE Resource Directory	2019-07-08 76 pages	AD Evaluation for 49 days Submitted to IESG for Publication: Proposed Standard	
draft-ietf-core-senml-data-ct-00 SenML Data Value Content-Format Indication	2019-08-29 6 pages	I-D WG Document	Exists
draft-ietf-core-senml-etch-05 FETCH & PATCH with Sensor Measurement Lists (SenML)	2019-08-17 10 pages	IESG Evaluation::Revised I-D Needed for 18 days Submitted to IESG for Publication: Proposed Standard Reviews: genart, iotdir, opsdir, secdir	
draft-ietf-core-senml-more-units-00 Additional Units for SenML	2019-09-02 7 pages	I-D WG Document	Exists
draft-ietf-core-sid-07 YANG Schema Item iDentifier (SID)	2019-07-08 29 pages	I-D WG Document	Exists
draft-ietf-core-yang-cbor-11 CBOR Encoding of Data Modeled with YANG	2019-09-11 44 pages New	I-D WG Document	Exists

Document	Date	Status	
draft-ietf-core-yang-library-00 Constrained YANG Module Library	2019-07-24 15 pages	I-D WG Document	Exists
RFC 6690 (was draft-ietf-core-link-format) Constrained RESTful Environments (CoRE) Link Format	2012-08 22 pages	Proposed Standard RFC	
RFC 7252 (was draft-ietf-core-coap) The Constrained Application Protocol (CoAP)	2014-06 112 pages	Proposed Standard RFC Updated by RFC7959, RFC8613	
RFC 7390 (was draft-ietf-core-groupcomm) Group Communication for the Constrained Application Protocol (CoAP)	2014-10 46 pages	Experimental RFC	
RFC 7641 (was draft-ietf-core-observe) Observing Resources in the Constrained Application Protocol (CoAP)	2015-09 30 pages	Proposed Standard RFC Updated by RFC8323	
RFC 7959 (was draft-ietf-core-block) Block-Wise Transfers in the Constrained Application Protocol (CoAP)	2016-08 37 pages	Proposed Standard RFC Updated by RFC8323, RFC8323	[1]
RFC 8075 (was draft-ietf-core-http-mapping) Guidelines for Mapping Implementations: HTTP to the Constrained Application Protocol (CoAP)	2017-02 40 pages	Proposed Standard RFC	
RFC 8132 (was draft-ietf-core-etch) PATCH and FETCH Methods for the Constrained Application Protocol (CoAP)	2017-04 21 pages	Proposed Standard RFC	[1]
RFC 8323 (was draft-ietf-core-coap-tcp-tls) CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets	2018-02 54 pages	Proposed Standard RFC	
RFC 8428 (was draft-ietf-core-senml) Sensor Measurement Lists (SenML)	2018-08 54 pages	Proposed Standard RFC	
RFC 8516 (was draft-ietf-core-too-many-reqs) "Too Many Requests" Response Code for the Constrained Application Protocol	2019-01 6 pages	Proposed Standard RFC	
RFC 8613 (was draft-ietf-core-object-security) Object Security for Constrained RESTful Environments (OSCORE)	2019-07 94 pages	Proposed Standard RFC	

- Supporting organizations
    - CORE is an IETF WG.
- Domain:
    - 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 and applications edge of the vertical axis
- Application area:
    - CORE WG is focusing on horizontal industry.

- Scope:
    - 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:
    - 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:
    2. Development Status:

The WG will have five deliverables:

1. Republishing a version of RFC 8152 suitable for advancement to Internet Standard.
2. Use of Hash-based Signature algorithms in COSE using draft-housley-suit-cose-hash-sig as a starting point (Informational).
3. Placement of X.509 certificates in COSE messages and keys using draft-schaad-cose-x509 as a starting point (Informational).

4. Define the algorithms needed for W3C Web Authentication for COSE using draft-jones-webauthn-cose-algorithms and draft-jones-webauthn-secp256k1 as a starting point (Informational).
5. Define a small number of hash functions for X.509 certificate thumbprints and for indirect signing (for SUIT) (Informational).

3. Compliance:

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

4. Openness:

- Open to public.

5. Ratification process:

- Done by members and open for consultation from external parties.
- Open process for all parties interested in the ratification.

- Interoperability level:
  - Syntactical interoperability.
  - Technical interoperability.
- Standards:
  - 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/

Document	Date	Status
Active Internet-Drafts		
draft-ietf-cose-hash-algs-01 CBOR Object Signing and Encryption (COSE): Hash Algorithms	2019-06-10 10 pages	I-D Exists In WG Last Call
draft-ietf-cose-hash-sig-03 Use of the Hash-based Signature Algorithm with CBOR Object Signing and Encryption (COSE)	2019-05-10 22 pages	AD Evaluation for 59 days Submitted to IESG for Publication: Proposed Standard
draft-ietf-cose-rfc8152bis-algs-05 CBOR Object Signing and Encryption (COSE): Initial Algorithms	2019-09-11 44 pages New	I-D Exists WG Document
draft-ietf-cose-rfc8152bis-struct-06 CBOR Object Signing and Encryption (COSE): Structures and Process	2019-09-11 86 pages New	I-D Exists WG Document
draft-ietf-cose-webauthn-algorithms-01 COSE and JOSE Registrations for WebAuthn Algorithms	2019-07-08 10 pages	I-D Exists WG Document
draft-ietf-cose-x509-04 CBOR Object Signing and Encryption (COSE): Headers for carrying and referencing X.509 certificates	2019-09-12 9 pages New	I-D Exists WG Document
RFC 8152 (was draft-ietf-cose-msg) CBOR Object Signing and Encryption (COSE)	2017-07 121 pages	Proposed Standard RFC
RFC 8230 (was draft-jones-cose-rsa) Using RSA Algorithms with CBOR Object Signing and Encryption (COSE) Messages		

- Supporting organizations
  - COSE is an IETF WG.
- Domain:
  - 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 and applications edge of the vertical axis

- Application area:
  - COSE WG is focusing on horizontal industry.
- Scope:
  - 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:
  - 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/about/

  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.
- Problem statement: This effort will establish the deployment environment and deterministic network requirements.
- 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:

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

- Readiness:

  1: Adoption:

  - Working Group not officially formed.

2. Development Status:

Date	Milestone
Jul 2019	Re-charter or close
Apr 2019	Submit YANG model (Standards Track)
Dec 2018	Submit data flow information model (informational)
Nov 2018	Submit data plane specification (Standards Track)
Nov 2018	Finalize problem statement (informational)
Sep 2018	WG adoption of YANG model
Apr 2018	Submit architecture (Standards Track)
Mar 2018	Finalize use cases (informational)

3. Compliance
    - Not IETF responsibility.

4. Openness:
    - Open to public.

5. Ratification process:
    - Open process for all parties interested in the ratification.

- Interoperability level:
    - Syntactical interoperability.
    - Technical interoperability.
    - Semantic interoperability.
- Standards:

Document	Date	Status	
Active Internet-Drafts			1
draft-ietf-detnet-bounded-latency-00 DetNet Bounded Latency	2019-07-24 27 pages	I-D Exists WG Document	
draft-ietf-detnet-data-plane-framework-02 DetNet Data Plane Framework	2019-09-13 26 pages New	I-D Exists WG Document	
draft-ietf-detnet-flow-information-model-05 DetNet Flow Information Model	2019-09-12 22 pages New	I-D Exists WG Document	
draft-ietf-detnet-ip-01 DetNet Data Plane: IP	2019-07-01 22 pages	I-D Exists WG Document	
draft-ietf-detnet-ip-over-mpls-01 DetNet Data Plane: IP over MPLS	2019-07-01 12 pages	I-D Exists WG Document	
draft-ietf-detnet-ip-over-tsn-00 DetNet Data Plane: IP over IEEE 802.1 Time Sensitive Networking (TSN)	2019-05-06 21 pages	I-D Exists WG Document	
draft-ietf-detnet-mpls-01 DetNet Data Plane: MPLS	2019-07-01 30 pages	I-D Exists WG Document	
draft-ietf-detnet-mpls-over-tsn-00 DetNet Data Plane: MPLS over IEEE 802.1 Time Sensitive Networking (TSN)	2019-05-06 23 pages	I-D Exists WG Document	
draft-ietf-detnet-mpls-over-udp-ip-01 DetNet Data Plane: MPLS over UDP/IP	2019-07-01 8 pages	I-D Exists WG Document	
draft-ietf-detnet-security-05 Deterministic Networking (DetNet) Security Considerations	2019-08-29 44 pages	I-D Exists WG Document	
draft-ietf-detnet-tsn-vpn-over-mpls-00 DetNet Data Plane: IEEE 802.1 Time Sensitive Networking over MPLS	2019-05-06 17 pages	I-D Exists WG Document	
draft-ietf-detnet-yang-03 Deterministic Networking (DetNet) Configuration YANG Model	2019-07-08 38 pages	I-D Exists WG Document	
RFC 8557 (was draft-ietf-detnet-problem-statement) Deterministic Networking Problem Statement	2019-05 11 pages	Informational RFC	
RFC 8578 (was draft-ietf-detnet-use-cases) Deterministic Networking Use Cases	2019-05 97 pages	Informational RFC	1

- Supporting organizations:
    - DetNet is an IETF WG.
- Domain:
    - 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 and applications edge of the vertical axis
- Application area:
    - DetNet WG is focusing on horizontal industry.
- Scope:
    - 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:
    - 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:

  - Widely used in the industry.

  2. Development Status:

  Concluded/completed WG

- 3. Compliance:
  - Not IETF responsibility.

  4. Openness:

  - Open to public.

  5. Ratification process:

  - Open process for all parties interested in the ratification.

- Interoperability level:
  - Syntactical interoperability.
  - Technical interoperability.
  - Semantic interoperability.
- Standards:

RFC 7925 (was draft-ietf-dice-profile) Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things	2016-07 61 pages	Proposed Standard RFC

- Supporting organizations
  - Dice is a concluded/completed IETF WG.
- Domain:
  - 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 and applications edge of the vertical axis.
- Application area:
  - Dice WG focused on horizontal industry.
- Scope:
  - 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:
  - Access of published (RFCs) and non-published (Internet draft) specifications for members and non-members is open and free of payment.

5.2.17 IRTF (Internet Research Task Force)

The Internet Research Task Force (IRTF) promotes research of importance to the evolution of the Internet protocols, applications, architecture and technology, see: https://irtf.org/.

The Internet Research Task Force (IRTF) focuses on longer term research issues related to the Internet while the parallel organization, the Internet Engineering Task Force (IETF), focuses on the shorter term issues of engineering and standards making.

The IRTF is comprised of a number of focused and long-term Research Groups. These groups work on topics related to Internet protocols, applications, architecture and technology. Research Groups have the stable long-term membership needed to promote the development of research collaboration and teamwork in exploring research issues. Participation is by individual contributors, rather than by representatives of organizations.

T2T (Thing to Thing) RG

- Description:

  The Thing-to-Thing Research Group (T2TRG) will investigate open research issues in turning a true "Internet of Things" into reality, 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 the T2TRG are on issues that touch opportunities for standardization in the IETF, i.e., it will 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.

  - Areas of Interest
    - Understanding the motivation for single-purpose silos and gateways; facilitating a move towards small pieces loosely joined (hence "thing-to-thing"); enabling 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 models, formats, and semantics
  - More exploratory areas of interest include:
    - Operating "things" that have multiple masters/stakeholders (including understanding role definitions of devices, owners, operators, etc.)
    - Exploring the duality of state- and event-based approaches
    - Aspects of distribution (cf. "fog computing"); reliability and scalability considerations
    - Containerization and other forms of mobile code
- Readiness:

  1. Adoption:
     - Well adopted
  2. Development Status:
     - RFC published, see: "Internet of Things (IoT) Security: State of the Art and Challenges", RFC 8576, see: https://datatracker.ietf.org/doc/rfc8576/
     - On edge computing, there is an Internet draft being active: "IoT Edge Challenges and Functions", see: https://datatracker.ietf.org/doc/html/draft-irtf-t2trg-iot-edge-02
  3. Compliance:
  4. Openness:
     - Open to public.

5. Ratification process:
    - Done by members and open for consultation from external parties.
    - Open process for all parties interested in the ratification.

- Interoperability level:
    - Syntactical interoperability.
    - Technical interoperability.
    - Semantic interoperability.
- Standards:
    - The T2T RG is an IRTF Research Group that will be using and providing input mainly to IETF, but also to the IOT and edge computing research community. Produced one RFC: "Internet of Things (IoT) Security: State of the Art and Challenges", RFC 8576, see: https://datatracker.ietf.org/doc/rfc8576/
- Supporting organizations:
    - T2T RG is belonging to IRTF that is closely cooperating with the IETF and it represents the research activities of IETF.
- Domain:
    - 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:
    - IRTF T2T RG is focusing on horizontal industry.
- IPR Policy Available:
    - The IRTF follows the IETF Intellectual Property Rights (IPR) disclosure rules, see: https://irtf.org/ip. . 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: https://www.ietf.org/ipr/file-disclosure

  See RFC 8179 (BCP 79) for definitions of "IPR" and "contribution" and for the detailed rules (substituting "IRTF" for "IETF", see: https://ietf.org/
- Specification Access:
    - Access of published (RFCs) and non-published (Internet draft) specifications for members and non-members is open and free of payment.

COIN (Computing in the Network) RG

- Description:

  The COIN proposed research group (COINRG) will explore existing research and foster investigation of "Compute In the Network" and resultant impacts to the data plane, see: https://datatracker.ietf.org/rg/coinrg/about/. The goal is to investigate how to harness and to benefit from this emerging disruption to the Internet architecture to improve network and application performance as well as user experience. COIN will encourage scrutiny of research solutions that comprehend the re-imagining of the network to be a place where routing, compute, and storage blend.

  COIN will address both controlled environments such as DCN and the ongoing shift from data center (DC) toward edge computing and will debate whether this shift can be viewed as a cloud continuum. COIN specifically will focus on the evolution necessary for networking to move beyond packet interception as the basis of network computation. While existing DCs employ rudimentary languages for programming switch, richer programmability is required to support emerging workloads, such as edge network analytics, machine learning and deep learn. Such applications not only need access to more general-purpose languages, but also need to operate in conjunction with local and remote caches, dynamic control points, and data stewardship.

  Orchestration of end-to-end resources between the DC network and the edge is another key topic to address in COIN. In particular, the RG will examine orchestration with increasingly heterogeneous distributed components and draw inspiration from current approaches (e.g., Kubernetes, Swarm) that are likely to need updating, extending, and/or simplifying in multi-domain network environments.

  Use-case-driven requirements, gathered from next-generation applications and services (e.g., video streaming, immersive AR/VR, autonomous/connected vehicles, industrial IoT), may lead to new architectures, which employ new ways to perform functional distribution and leverage co-design of layered approaches.

  In order to achieve its goals, COIN will expose and advance research on distributed, decentralized networks and resources required by DC, edge and ambient computing. COIN will investigate the implications of increased heterogeneity and limitations that arise if/when DC and edge computing employ a common architecture, programmable networks and API and interchangeable functionality in the Internet. An assumption will be that to improve Internet performance, the network, compute and storage resources must work jointly in close partnership throughout the network, while servicing data-intensive distributed applications.

  SCOPE of the COINRG:

  1. Research on solutions to use programmable network devices, languages and abstractions to implement network functions for improved Internet performance.
  2. Research on use case driven requirements analysis: the cloud continuum from the data center to edge networks and beyond including in-network computing using programmable switches. Identify potential benefits to these networks from in-network functionality, including but not limited to compute, cache, manage, control, etc.
  3. Research on novel architectures, data-plane abstractions and new network protocol designs to efficiently federate decentralized computing resources, across the infrastructure regardless of where in the network the compute is placed (the DC, the core, the edge, and even in the end-user devices).
  4. Research on potential new transport protocol, new privacy and security mechanisms required or enabled by in-network compute.

- Readiness:

1. Adoption:

- Well progressing

2. Development Status:

Date	Milestone
Nov 2020	Work toward defining a COIN scope appropriate for the IRTF, within which new architectures, mechanisms and protocols can be proposed
Apr 2020	Identify COIN network-related eco-system dependencies
Apr 2020	Target COIN case studies, from architecture, implementation and use case standpoints draft-montpetit-coin-xr draft-he-coin-managed-networks
Apr 2020	Discuss/catalog COIN requirements and implications for network elements (including network services, network SW stacks, network HW design, etc.) draft-mcbride-edge-data-discovery-overview draft-he-coin-managed-networks draft-kunze-coin-industrial-use-cases
Dec 2019	Articulate COIN challenges draft-liu-coinrg-requirement draft-kutscher-coinrg-dir
Dec 2019	Capture the SoTA of the COIN landscape draft-kutscher-coinrg-dir

3. Compliance:

4. Openness:

- Open to public.

5. Ratification process:

- Done by members and open for consultation from external parties.
- Open process for all parties interested in the ratification.

- Interoperability level:

1. Syntactical interoperability.
2. Technical interoperability.
3. Semantic interoperability.

- Standards:
  - The COIN RG is an IRTF Research Group that will be using and providing input mainly to IETF, but also to the edge computing research community.
- Supporting organizations:
  - COIN RG is belonging to IRTF that is closely cooperating with the IETF and it represents the research activities of IETF.
- Domain:
  - 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:
  - IRTF COIN RG is focusing on horizontal industry.

- IPR Policy Available:
  - The IRTF follows the IETF Intellectual Property Rights (IPR) disclosure rules, see: https://irtf.org/ip. . 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: https://www.ietf.org/ipr/file-disclosure

  See RFC 8179 (BCP 79) for definitions of "IPR" and "contribution" and for the detailed rules (substituting "IRTF" for "IETF", see: https://ietf.org/
- Specification Access:
  - Access of published (RFCs) and non-published (Internet draft) specifications for members and non-members is open and free of payment.

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

- Description:

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 "Internet of things (IoT) and smart cities and communities (SC&C)", established in June 2015, is the central venue for IoT and smart cities standardization activities within ITU-T. Note that activities related to edge computing for the IoT are as well addressed.

SG20 addresses the standardization requirements of Internet of Things (IoT) and smart cities and communities (SC&C).

SG20, via the Joint Coordination Activity on Internet of Things and Smart Cities & Communities whose supervision is ensured by SG20, maintains the coordination of IoT and smart cities & communities related studies across the various involved ITU-T Study Groups as well as with external SDOs, Alliances and Consortia.

Specific study items (a not exhaustive list) of SG20 include:

- 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 requirements, capabilities and architectural frameworks across verticals, platforms, end-to-end architectures and protocols for IoT, mechanisms for the interoperability and interworking of IoT applications, networks and datasets employed by verticals.
- Development of international standards that leverage IoT technologies to address urban-development challenges, assess and evaluate smart cities and communities .
- IoT research and emerging technologies incl. - but not limited to - **Edge Computing**, Blockchain, Digital Twin, AI/ML, Big Data and Analytics **for IoT**.
- IoT trust, privacy and security.
- IoT identification.
- IoT semantics.
- IoT analytics, sharing, processing and management
- IoT accessibility

In terms of IoT and smart cities & communities, it has to be noted by the way that different ITU-T study groups have some related studies in the context of their specific areas of competence and also considering the current pervasive impact of digital transformation (largely enabled via the support of IoT related technologies) in all sectors of economy and society. Specific mention is deserved for ITU-T SG17 (general and vertical-specific security aspects of IoT and related technologies), ITU-T SG16 (multimedia aspects of IoT and related technologies), ITU-T SG13 and SG11 (network aspects of IoT and related technologies, including Edge Computing).

An ITU-T Focus Group which has been particularly relevant for IoT and smart cities & communities pre-standardization over the most recent years has been the Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities (FG-DPM) [established 2017-03, terminated 2019-07], most of its deliverables having been transferred and progressed by SG20 at the FG closure time.

A domain-specific international standardization coordination activity ensured by ITU-T is the **Collaboration on ITS Communication Standards (CITS)** (*https://www.itu.int/en/ITU-T/extcoop/cits/Pages/default.aspx*), whose intent is to provide a globally recognized forum for the coordination of an internationally accepted, globally harmonized set of Intelligent Transportation Systems (ITS) communication standards of the highest quality in the most expeditious manner possible to enable the rapid deployment of fully interoperable ITS communication-related products and services in the global marketplace.

It has also to be noted the UN initiative called **"United for Smart Sustainable Cities (U4SSC)"** *(https://www.itu.int/en/ITU-T/ssc/united/Pages/default.aspx)*, coordinated by ITU, UNECE and UN-Habitat, and supported by CBD, ECLAC, FAO, UNDP, UNECA, UNESCO, UNEP, UNEP-FI, UNFCCC, UNIDO, UNOP, UNU-EGOV, UN-Women and WMO. The U4SSC goal is to achieve Sustainable Development Goal 11: "Make cities and human settlements inclusive, safe, resilient and sustainable"

Note about ITU-T activities on IoT and smart cities & communities before October 2015

The IoT related specifications published before October 2015 by ITU-T, and the main IoT related activities of ITU-T till that time, involved Study Group 11, Study Group 13, Study Group 16 and Study Group 17:

- SG11 focused on the interoperability, protocol and testing aspects of IoT;
- SG13 mainly focused on the network aspects of IoT;
- SG16 mainly focused on the application aspects of IoT;
- SG17 focused on the security aspects of IoT.

Smart cities related activities were progressed before October 201within specific ITU-T Focus Groups which produced a set of technical reports and technical specifications, most of which were transformed into Supplements and ITU-T Recommendations (e.g. ITU-T L.1603 series: KPIs for Smart Sustainable Cities). The main Focus Groups involved in IoT and smart cities issues till October 2015 were: the Focus Group on M2M Service Layer, the Focus Group on Smart Water Management and the Focus Group on Smart Sustainable Cities.

Additional IoT activities were progressed within Study Group 15 (Smart Grid and Home Network aspects) and the Collaboration on ITS Communication Standards.

- Readiness:

1. Adoption:
   - 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:
   - 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:
  - Technical interoperability/Syntactical interoperability (according to the particular specification).

    NOTE – Some specific ongoing studies are considering Semantic interoperability aspects.

- Standards:
  - Various IoT and smart cities & communities standards have been proposed in published specifications (and others are considered in some ongoing studies).
  - Some published specifications on IoT and smart cities & communities use and integrate standards and protocols developed by other SDOs (and other SDOs' standards and protocols are considered in some ongoing studies). A specific mention to the transposition of various oneM2M specifications into ITU-T specifications (Recommendations, Supplements).

- Supporting organizations
    - 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:
    - Most of the activities target the market without specific focus on consumer versus industrial internet.
    - Both sides of the technology domain are targeted, according to the particular specification.
- Application area:
    - 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:
    - 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:
    - ITU / ISO / IEC code of practice.

      All details can be found at http://www.itu.int/en/ITU-T/ipr/Pages/default.aspx.
- Specification Access:
    - 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.

5.2.19 ISO/IEC JTC1

- 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.

ISO/IEC JTC 1 ISO/IEC JTC 1 WG10 (IoT) / SC 41

The ISO/IEC JTC 1 WG10 (IoT) is denoted as ISO/IEC JTC 1/SC 41 since May 2017

- The ISO/IEC JTC 1 WG10 (IoT) has prepared a Strategic business plan but it will be confirmed at the upcoming JTC1 meeting in October 2012 in China. Until then the WG has the mandate to develop one standard which has got the following title and scope:
- The ISO/IEC JTC 1 WG10 (IoT) is denoted as ISO/IEC JTC 1/SC 41 since May 2017

  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 a conceptual to business specific IoT Architectures.

ISO/IEC JTC 1/SC 38 - Cloud computing and distributed platforms[1]

Standardization in the areas of Cloud Computing and Distributed Platforms including:

- Foundational concepts and technologies,
- Operational issues, and
- Interactions among Cloud Computing systems and with other distributed systems

SC 38 serves as the focus, proponent, and systems integration entity on Cloud Computing, Distributed Platforms, and the application of these technologies. SC 38 provides guidance to JTC 1, IEC, ISO and other entities developing standards in these areas.

[1] https://www.iso.org/committee/601355.html

- Readiness:

  1. Adoption:
     - 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:
     - 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:
  - Syntactical interoperability.
  - Technical interoperability.
- Standards:
  - ISO SC41
    - 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.
  - ISO SC38
    - ISO/IEC TR 23188:2020 Information technology — Cloud computing — Edge computing landscape
      - This document examines the concept of edge computing, its relationship to cloud computing and IoT, and the technologies that are key to the implementation of edge computing. This document explores the following topics with respect to edge computing:
        - concept of edge computing systems;
        - architectural foundation of edge computing;
        - edge computing terminology;
        - software classifications in edge computing, e.g. firmware, services, applications;
        - supporting technologies, e.g. containers, serverless computing, microservices;
        - networking for edge systems, including virtual networks;
        - data, e.g. data flow, data storage, data processing;

- management, of software, of data and of networks, resources, quality of service;
- virtual placement of software and data, and metadata;
- security and privacy;
- real time;
- mobile edge computing, mobile devices.

- Supporting organizations:
- Domain:
  - 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:
  - The ISO/IEC JTC 1 standards document will benefit horizontal industries.
- 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 thrugh ISO.
  - Members of a National Standardization Body who are 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.

5.2.20 M2.COM

- Description:

  M2.COM is a brand new platform form factor for sensors. It adopts the standardized, frequently used M.2 form factor and is defined as an evolutionary module that combines general wireless connectivity with additional built-in computing ability powered by MCU.

- Readiness:

  1. Adoption:
  2. Development Status:
     - Available
  3. Compliance:
  4. Openness:
     - Open by formal membership.
  5. Ratification Process:

- Interoperability level:
  - Technical
- Standards:
  - Adopts the type 2230 M.2 form factor and various interfaces like USB, I2S, I2C, SDIO and will support different wireless communication standards.
- Member organizations:
  - Advantech, ARM, Bosch, Texas Instruments, Sensirion.
- Domain:
  - More industrial than consumer; Connectivity layer, but also computing platform.
- Application area:
  - Sensor applications in any area.
- Scope:
  - Infrastructure knowledge area Sensor, Communication and Connectivity knowledge area.
- IPR Policy:
- Specification Access:
  - Public available http://www.m2com-standard.org/

5.2.21 MIPI Alliance

- Description:

MIPI Alliance Overview

MIPI Alliance is a global, collaborative organization comprised of companies that span the mobile ecosystem and are committed to defining and promoting interface specifications for mobile devices. All companies in the mobile device industry are encouraged to join, including semiconductor companies, software vendors, IP providers, peripheral manufacturers, test labs and end product OEMs. Today, more than 275 member companies actively participate in the Alliance, developing interface specifications which drive consistency in processor and peripheral interfaces, promoting reuse and compatibility in mobile devices.

MIPI Alliance Specification Scope

- MIPI specifications may impact both hardware and software in mobile devices.
- From a hardware perspective, a processor or system-on-a-chip typically has several ports or busses which interface to a variety of peripherals such as displays, cameras, memory, or communications devices. In addition, there may be interconnections among the peripheral devices. The MIPI Alliance is constantly analysing these interconnect scenarios, and pursuing MIPI Specifications in those cases where standardization is likely to benefit the industry.
- MIPI Specifications address only the interface technology, such as signalling characteristics and protocols. MIPI Specifications do not standardize entire application processors or peripherals. Products which utilize MIPI Specifications will retain many differentiating features. The MIPI Alliance does not seek to "commoditize" or drive pin-compatible, drop-in replacements among these products. Rather, we seek to create standards for these products to communicate with each other. By enabling products which share common MIPI interfaces, system integration is likely to be less burdensome than in the past.

MIPI Alliance key links:

- MIPI Alliance: http://mipi.org
- Member company directory: http://mipi.org/member-directory
- MIPI Alliance Specification information: http://mipi.org/specifications

MIPI Alliance in IoT

MIPI Alliance Specifications are widely adopted in not only the mobile device industry, but in IoT space as well. This includes the following specifications:

- MIPI I3C Specification (Sensors)
  - I3C Whitepaper is available here
  - MIPI I3C is a bus interface for connecting sensors to an application processor. It is a core sensor integration technology that can combine multiple sensors from different vendors in a device to streamline integration and improve cost efficiencies. It gives developers unprecedented opportunity to craft innovative designs for any mobile product, from smartphones, to wearables, to safety systems in automobiles.
  - MIPI I3C can integrate mechanical, motion, biometric and environmental, and any other type of sensor. It incorporates key attributes of the traditional I2C and SPI interfaces to provide a new, unified, high-performing, very low power solution. The technology is implemented on a standard CMOS I/O. It uses a two-wire interface, which reduces pin count and signal paths to offer system designers less complexity and more flexibility. It can also be used as a sideband interface to further reduce pin count. MIPI I3C supports a minimum data rate of 10 Mbps with options for higher performance high data rate modes, offering a substantial leap in performance and power efficiency compared with previous options
- MIPI Camera Serial Interface (CSI-2) Specification
  - CSI-2 Specification brief is available: https://mipi.org/sites/default/files/files/MIPI%20CSI-2%20Specification%20Brief.pdf

        - The MIPI® Alliance Camera Working Group has created a clear design path that is sufficiently flexible to resolve not just today's bandwidth challenge but "features and functionality" challenges of an industry that manufactures more than a billion handsets each year for a wide spectrum of users, applications and cost points.
        - The latest Camera Serial Interface 2 Specication (CSI-2 v1.3) o ers higher interface bandwidth and greater channel layout exibility than its predecessor. It introduces C-PHY1.0, a new PHY that MIPI Alliance released in September 2014, as well as support for the previous version's D-PHY1.2 interface. Both PHY options improve skew tolerance and provide higher data rates. Both are serial interfaces that address many of the problems of parallel interfaces, which consume relatively large amounts of power, are difficult to expand and can be proprietary.
    - MIPI Display Serial Interface (DSI) Specification
        - The Display Serial Interface Specification defines protocols between a host processor and peripheral devices using a D-PHY physical interface. The DSI specification builds on existing specifications by adopting pixel formats and command set defined in MIPI Alliance specifications for Display Pixel Interface 2 (DPI-2) and Display Command Set (DCS)
        - DSI defines interface protocols formatting link management, signal timing relationships and error handling. This specification refers to D-PHY Specification for electrical specifications. Device usage of auxiliary buses such as I2C or SPI, while not precluded by this specification, are out of scope.
        - The DSI specification defines a high-speed serial interface between a peripheral, such as an active-matrix display module, and a host processor in a mobile device. By standardizing this interface, components may be developed that provide higher performance, lower power, less electromagnetic interference and fewer pins than current devices, while maintaining compatibility across products from multiple vendors.
    - MIPI RF Front End (RFFE) Specification
        - RFFE Specification brief is available here.
        - The *MIPI Alliance Specification for RF Front-End Control Interface (*RFFE) was developed to offer a common and widespread method for controlling RF front-end devices. There are a variety of front-end devices, including Power Amplifiers (PA), Low-Noise Amplifiers (LNA), filters, switches, power management modules, antenna tuners and sensors. These functions may be located either in separate devices or integrated into a single device, depending on the application.
        - RFFE provides a low-complexity solution to meet the cost and performance targets of RF front-end components. It offers extensibility from simple configurations with one Slave on a single bus, all the way to complex configurations with many Slaves on a single bus, or distributed on multiple buses. This eases both the RF and front-end module design by requiring a mobile terminal to support only a single control interface. Ideally, this leads to a broader range of control-compatible components, and to larger markets for front-end devices.
- Readiness:

    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.)
            - This includes a Product Registry program which lists products that have been evaluated by Members, through either self-testing or a qualified independent test lab. The MIPI Product Registry is not a certification or compliance program.

    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
        - Exceptions are cases where liaison agreement is in place with external parties

- Interoperability level::
    - Technical interoperability
- Standards:
    - MIPI Alliance specifications are developed by MIPI Alliance contributor members.
- Supporting organizations
    - N/A
- Domain:
- Application area:
- Scope:
    - Communication and Connectivity knowledge area:
    - Integration/Interoperability knowledge area:
    - Devices and sensor technology knowledge area:
- IPR Policy Available:
    - With MIPI membership, the license is royalty-free inside mobile terminals and accessories as defined, and outside, RAND licensing applies. MIPI Alliance membership agreement is available: https://mipi.org/sites/default/files/MIPI-MA-2006.pdf
- Specification Access:
    - MIPI Alliance members have access to all published specifications. Contributor-level MIPI Alliance members have access to draft specifications. Select software specifications are publicly available with legal agreement.

5.2.22 NFC (Near Field Communication) Forum

- Description:

The NFC Forum (http://nfc-forum.org/) brings the convenience of NFC technology to life by empowering organizations to deliver secure, tap-based interactions with an intuitive, reliable experience to users around the globe.

The goals of the NFC Forum are to:

- Develop specifications and test mechanisms that ensure consistent, reliable transactions worldwide across all three modes of NFC
- Take a leadership role in the industry to ensure NFC technology can routinely deliver a positive user experience
- Educate enterprises, service providers, and developers about the benefits of NFC technology to ensure growth in end user adoption
- Establish the NFC Forum and NFC technology brands as well recognized and utilized marks

The NFC Forum provides a highly stable framework for extensive application development, seamless interoperable solutions, and security for NFC-enabled transactions. The NFC Forum has organized the efforts of dozens of member organizations by creating Committees and Working Groups.

In June 2006, only 18 months after its founding, the Forum formally outlined the architecture for NFC technology. The Forum has released 16 specifications to date. The specifications provide a "road map" that enables all interested parties to create powerful new consumer-driven products.

- Readiness:
  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:
  - Technical interoperability
  - Syntactical interoperability
- Standards:
  - NFC Forum develops its own specifications complementing many popular consumer level wireless technologies by utilizing key elements in existing standards for contactless card technology (ISO/IEC 14443 A&B, ISO/IEC 15693 and JIS-X 6319-4).
- Supporting organizations
  - See at http://nfc-forum.org/about-us/our-members/
- Domain:
  - Consumer – Connectivity quadrant
- Application area:
  - Horizontal/Telecommunication
- Scope:
  - Communication and Connectivity knowledge area
- IPR Policy Available:
  - RAND, refer to http://nfc-forum.org/wp-content/uploads/2013/11/NFC-Forum-IPR-Policy.pdf
- Specification Access:
  - Public specifications can be purchased by non-members
  - Public specifications are available to all NFC Forum members
  - Draft specifications are available for Associate, Principal and Sponsor Members

5.2.23 OCF (Open Connectivity Foundation)

- Description:

  The Open Connectivity Foundation, an entity whose goal will be to help unify IoT standards so that companies and developers can create IoT solutions and devices that work seamlessly together. Via cross-industry collaboration, the OCF will work towards unlocking the massive opportunity of the future global IoT segment, accelerate industry innovation and help all developers and companies create solutions that map to a single, open IoT interoperability specification. Ultimately, with OCF specifications, protocols and open source projects, a wide-range of consumer, enterprise and embedded devices and sensors from a variety of manufacturers, can securely and seamlessly interact with one another.

  The OCF unifies the entirety of the former Open Interconnect Consortium with leading companies at all levels – silicon, software, platform, and finished-goods – dedicated to providing this key interoperability element of an IoT solution.

  The OCF's vision for IoT is that billions of connected devices (appliances, phones, computers, industrial equipment) will communicate with one another regardless of manufacturer, operating system, chipset or transport. With the OCF fulfilling this promise, anyone – from a large technology company to a maker in their garage – can adopt the open standards of OCF to innovate and compete, helping ensure secure interoperability for consumers, business, and industry.

- Readiness:

  1. Adoption:
     - Reference implementations.
  2. Development Status:
     - Approved with planned revisions.
  3. Compliance:
     - Formal certification process.
  4. Openness:
     - Open by formal membership.
  5. Ratification process:
     - Closed process done by members only with no consultation from external parties.

- Interoperability level:
  - Organisational interoperability. Note work is ongoing to interoperate through the OneM2M platform as well as across the OCF and AllSeen ecosystem.
- Standards:
- Combination of existing IETF and W3C standards with additional work.
- Supporting organizations
- Working with OneM2M.
- Domain:
  - Multiple domains – initial release has a consumer focus with a mix of connectivity and services.
- Application area:
  - Different specifications cover different areas. The initial focus is on Smart Home.
- Scope:
  - OCF covers all these 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:
  - FRANDz – Free licencing.
- Specification Access:
  - Specification open on OCF web site – free to access for all.

5.2.24 OneM2M

- Description:

  The text used in this section is based on: http://www.onem2m.org/about-onem2m/why-onem2m.

  oneM2M was launched in 2012. It is a global initiative (Partnership Project) that develops specifications to ensure the most efficient deployment of Machine-to-Machine (M2M) communications systems and the Internet of Things (IoT).

  oneM2M vision: A world of interoperable and secure IoT services where market adoption is easy and delivers benefits to society."

  oneM2M mission: "We are the global community that develops IoT standards to enable interoperable, secure, and simple-to-deploy services for the IoT ecosystem. oneM2M standards are open, accessible and internationally recognized."

  The goal of oneM2M is to develop technical specifications for a common M2M and IoT service layer. This can be embedded within hardware and software to connect the wide range of devices worldwide with IoT and M2M application servers.

  By bringing together more than 200 players from many diverse business domains, oneM2M ensures the global functionality of M2M and IoT and prevents the duplication of standardization effort.

  Work in oneM2M is contribution driven, by members in working groups of the technical plenary.

  oneM2M Technical Plenary:

  - Requirements and Domain Models (RDM) Working Group
  - System Design and Security (SDS) Working Group
  - Testing and Developers Ecosystem (TDE) Working Group

  oneM2M has been defining 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);
    - Interworking towards other technologies standards in the subject area and legacy technologies, making it applicable for brownfield environments.
    - Common use cases, terminal/module aspects, including Service Layer interfaces/APIs between:
      - Application and Service Layers;
      - Service Layer and communication functions.

- Readiness:

  1. Adoption:
     - 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 and compliance testing..
       - Since 2015 seven interop test events have been held, offering interoperability as well as conformance test sessions..
     - Formal certification process:
       - The aim of the oneM2M Certification program is to assure users that certified products and services meet oneM2M standard testing requirements that ensure interoperability. oneM2M Certification is a LOGO program, NOT a compulsory program.
       - The program was pioneered by the Telecommunication Technology Association (Korea), one of oneM2M's founding Partners. Since 2019, the program has been operated by the Global Certification Forum, which serves the mobile and IoT industry, with certification initiatives that verify the quality of the interoperability between mobile phones, wireless and IoT devices across different network elements and diverse vendor infrastructure.
         https://www.onem2m.org/harmonization-m2m/certifications
         https://www.globalcertificationforum.org/services/onem2m-standards-form2m-and-iot.html
  4. Openness:
     - Open to public.
  5. Ratification process:
     - Done by members and open for consultation from external parties.

- Interoperability level:
  - Syntactical interoperability.
  - Technical interoperability.
  - Semantic interoperability.
- Standards:
  - Find and download the full set of oneM2M Technical Specifications and work program deliverables developed by oneM2M members from the earliest to the most recent Release cycle at: https://www.onem2m.org/technical
- Supporting organizations:

  oneM2M is a partnership project the current partners are:
  - 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 India (TSDSI);

        - Telecommunications Technology Association (TTA);
        - Telecommunications Technology Committee (TTC);
    - Partner Type 2:
        - GlobalPlatform;
    - 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;
    - ITU-T SG20 has transposed the oneM2M Specifications in its Y.4500.xseries
    - 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:
    - 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:
        - oneM2M is not chartered to focus on a particular vertical industry. It shall provide standardized common service layer technologies that enables interoperability of applications across any domain
        - In order to enable a smooth standards based interworking with other domains Technical Specifications and Technical Reports have been developed for selected vertical domains (e.g. home, industrial, vehiclular, railway and smart cities) in detail to ensure the provided standard/technology fulfills the vertical requirements and interwork. More domains may be investigated in the future.
- IPR Policy Available:
    - http://www.onem2m.org/images/files/oneM2M_Partnership_Agreement.pdf.
- Specification Access:
    - oneM2M published documents available at: http://www.onem2m.org/technical/published-documents
    - oneM2M latest drafts available at: http://www.onem2m.org/technical/latest-drafts

5.2.25 OSGi Alliance

- Description:

  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:
  - 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:
    - 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:
    - 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
    - The Strategic members of the OSGi Alliance include: Adobe, Deutsche Telekom, Huawei, 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:
    - 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:
    - 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:
    - 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:
    - OSGi specifications are royalty free.
- Specification Access:
    - Publicly available specifications with reference implementations and compliance tests.
    - Various open source and commercial implementations exist and are adopted by the industry.

5.2.26 The Open Group / Open Platform 3.0

- Description:

  Details on Open Platform 3.0™ can be found via:
  http://www.opengroup.org/subjectareas/platform3.0.

  The purpose of The Open Group's Open Platform 3.0™ Forum is to help organizations to take advantage of the convergence of modern technologies like cloud computing, social computing, mobile computing, big data analytics, and the internet of things. The Forum is creating The Open Platform 3.0 Standard as an interoperability standard for digital platforms, so that enterprises can more easily use these technologies in business solutions. Digital platforms that conform to it will work together, so that enterprises can combine them to access different technologies to meet business needs. The standard is currently at an early stage of development. The Open Group has published a snapshot as an indication of what the eventual standard might be, and as an invitation for input and comment. Enterprises wishing to gain advance understanding of this emerging standard, and influence its development, should join the Open Platform 3.0 Forum.

- Readiness:

  1- Adoption:

  - Reference implementations (e.g., the one related to O-MI/O-DF standards[2])

  2- Development Status:

  3- Compliance:

  4- Openness:

  5- Ratification process:

  - Done by members and open for consultation from external parties + Open process for all parties interested in the ratification.

- Interoperability level:

  - Syntactical interoperability – Handle by Open Platform 3.0.
  - Technical interoperability – Handle by Open Platform 3.0.
  - Semantic interoperability – Handle by Open Platform 3.0.
  - Organisational interoperability – Handle by Open Platform 3.0.

- Standards:

  - Open Messaging Interface (O-MI) and Open Data Format (O-DF) standards[3,4] developed by the IoT Work Group of The Open Group. Those two standards were officially published by The Open Group in October 2014, and a first version of the reference implementation was released[5,6].
  - UDEF Standard.
  - Cloud Computing Governance Framework.
  - Open Business Data Lake.
  - IoT Open Lifecycle Management.

[2] http://otaniemi3d.cs.hut.fi/omi/node/html/webclient/index.html

[3] https://www2.opengroup.org/ogsys/catalog/C14B

[4] https://www2.opengroup.org/ogsys/catalog/C14A

[5] https://github.com/AaltoAsia/omi-java

[6] http://otaniemi3d.cs.hut.fi/omi/node/html/webclient/index.html

- Supporting organizations:
    - The Open Group.
- Domain:
    - The Open Group has already been included in the IoT SDO and Alliances Landscape.
- Application area:
    - The Open Platform 3.0 published The Nexus of Forces in Action[7] that describes 22 Business Use-Cases in various domains, including cross-domain (i.e., horizontal industry) scenarios and applications. The table given below provides insight into the Use Case titles. Considering those titles, it can be noted that Open Platform 3.0 is targeting all domains and horizontal applications mentioned in Figure 2 in Section 4.2.

Business Use Cases identified/targeted by Open Platform 3.0

	Title
Use Case 1	Retail Smart Store
Use Case 2	Sustainable Shopping and Restaurant Street
Use Case 3	Multi-Channel Marketing
Use Case 4	Supply Chain Store Brand Integration
Use Case 5	Multi-Channel Customer Service
Use Case 6	Social Gamification Orchestration
Use Case 7	Multi-Service Provisioning Orchestration
Use Case 8	Augmented Lifestyle Sensor Feedback
Use Case 9	Augmented Patient Care Sensor Feedback
Use Case 10	Open Government Data Interchange
Use Case 11	Incident Management
Use Case 12	Information Control
Use Case 13	E-Medical Data Access and Exchange
Use Case 14	Translational Research – Bench to Bedside
Use Case 15	Mobile Smart Charging
Use Case 16	Electric Vehicles Ecosystem
Use Case 17	Smart Buildings and Home Appliances
Use Case 18	Smart Retail Distribution
Use Case 19	Maintenance of Air Conditioning
Use Case 20	Safe Mobility
Use Case 21	Investments and Asset Management
Use Case 22	Open Innovation, Crowd-Sourcing, and -Funding

[7] https://www2.opengroup.org/ogsys/catalog/W145

- Scope:
    - Open Platform 3.0 will not be realized as a single product, such as a unique middleware or operating system, but by a number of components (both smart objects and services) working in combination; these may be supplied by different enterprises, including commercial companies, non-profit organizations, open source projects, governments, as well as from vertically oriented closed systems. As a result, Open Platform 3.0 addresses (on a more or less intensive scale) all the areas listed below:
        - 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:
            - Open Platform 3.0 will also integrate ongoing work carried out by The Open Group on Security and Privacy aspects, see: http://www.opengroup.org/subjectareas/security
- IPR Policy Available:
- Specification Access:
    - Any person interested in the Open Platform 3.0 initiative and related Work Groups (e.g., IoT Work Group, Cloud Computing, The Business Context for Open Platform 3.0) can register himself/herself to the following URL: http://www.opengroup.org/subjectareas/platform3.0

5.2.27 TMForum

- Description:

  TM Forum is a global industry association for digital business, connecting talented individuals, leading companies, and diverse ecosystems to accelerate our members' successful digital business transformation. The collective experience and interests of our member community comprised of tens-of-thousands of professionals within 900+ market-leading organizations drives everything we do, from thought-provoking research and publications, to practical guidance, collaboration programs, tools and best practices, hands-on events, and training for business and IT leaders.

  Three Strategic Programs – Agile Business and IT, Open Digital Ecosystem, and Customer Centricity – are the lenses through which the Forum delivers our collaboration programs, research, standards, events, and training to our members. These programs focus on a wide range of pressing digital industry topics – NFV/SDN, Internet of Everything (IoE), customer engagement, data analytics, and security and privacy to name a few – to address the three major challenges outlined above and enable our members to innovate faster, better, and more effectively than they could ever hope to achieve on their own.

  The TM Forum recognizes that business, technology, and market dynamics will require management requirements for complex IoE/IoT services that span "networks of ecosystems". "IoE Service Management" will be required in many dimensions – from customer to infrastructure across many ecosystems even as the rapid pace of innovation continues forcing on going adoption and adapting of best practices and standards.

  Addressing IoE Service Management in the broadest sense, the TM Forum has on going "best practices" work streams and proof –of-concept projects addressing both (1) functional capabilities that extend across "vertical "Smart X" ecosystems" and (2) "end-to-end" operational capabilities.

  "Vertical "Smart X" ecosystems" include Smart Cities Forum, Smart Health, Smart Finance, Smart Mobility, and Smart Climate.

  IoE Best Practices, standards, toolkits and collaborative work includes:

  - Customer Digital Experience.
  - Rest Based API's.
  - B2B2x Ecosystem Partnership Guide.
  - Platform Capabilities Architecture.
  - Digital Services Reference Architecture.
  - Privacy Dashboard.
  - Applied Frameworx for IoE Business Scenarios demonstrated via Catalyst showcase projects.

- Readiness:

  - Each work stream produces deliverables on a member-driven prioritization schedule to create a set of "living" artifacts that enable members to drive organization IT and Operational transformation and successfully build IoE/Digital Solution ecosystem-based solutions.

  Each deliverable artifact has its own lifecycle as described below:

  1. Adoption:

     - 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 IoE related specification.

  4. Openness:

     - Open by formal membership.

5. Ratification process:

- 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:
  - Organizational interoperability/Technical interoperability/Syntactical interoperability (according to the particular specification).

- Standards:
  - Various standards have been proposed in published specifications (and others are considered in some ongoing studies).

    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).

- Supporting organizations
  - Telecommunication Hardware and Software Providers.
  - Digital Service Providers, Network Providers, Application Provider, Integrators.
  - Member State entities (Government entities, Academies, Public Research).
  - Other National and Regional Entities.

- Domain:
  - Most of the activities target the market without specific focus on consumer versus industrial Internet.
  - Both sides of the technology domain are targeted, according to the particular specification.
  - Recommended placement is "north" of the axis center point.

- Application area:

  Regarding IoE, there are ongoing "best practices" work streams and proof –of-concept projects addressing both (1) functional capabilities that extend across "vertical "Smart X" ecosystems" and (2) "end-to-end" operational capabilities.

  "Vertical "Smart X" ecosystems" include Smart Cities Forum, Smart Health, Smart Finance, Smart Mobility, and Smart Climate.

  - IoE Best Practices, standards, toolkits and collaborative work includes:
  - Customer Digital Experience.
  - Rest Based API's.
  - B2B2x Ecosystem Partnership Guide.
  - Platform Capabilities Architecture.
  - Digital Services Reference Architecture.
  - Privacy Dashboard.
  - Applied Frameworx for IoE Business Scenarios demonstrated via Catalyst showcase projects.

- Scope:
  - 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:
    - Digital Services capability.
  - Integration/Interoperability knowledge area.
  - Applications knowledge area.
  - Infrastructure knowledge area.

    - IoT Architecture knowledge area:
        - Covers integrated/complete IoE specification solutions, including architecture descriptions based on IoE Business Scenarios.
    - Devices and sensor technology knowledge area.
    - Security and Privacy knowledge area.
- IPR Policy Available:

    11. TM Forum Code of Practice/Policies
    12. https://www.tmforum.org/resources/tm-forum-operating-docs/policy-on-intellectual-property-rights/.

- Specification Access:
    - Published specifications: Accessible to members and non-members according to the particular specification and associated policy.
    - Non-published specifications: freely accessible to members only; not accessible to non-members.

5.2.28 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:
        - Reference implementations.
    2. Development Status:
        - Approved with planned revisions.
    3. Compliance:
        - Formal certification process.
    3. Openness:
        - Open by formal membership.
    5. Ratification process:
        - Closed process done by members only with no consultation from external parties.
- Interoperability level:
    - Technical interoperability.
- Standards:
    - Original standard developed by Weightless.
- Scope:
    - 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.

5.2.29 UDG Alliance

- Description:

  UDG Alliance is an alliance developing a multi-protocol framework of IoT interoperability. It enables the integration and interoperability among over 40 IoT standards. It enables interoperability among various IP and non-IP based IoT standards and communication protocols.

- Readiness:

  1. Adoption:
     - Reference implementations; used by several European research projects.

  2. Development Status:
     - Approved with planned revisions.

  3. Compliance
     - With over 40 IoT standards.

  4. Openness
     - Reserved to the UDG Alliance members.

  5. Ratification process:
     - Closed process done by members only with no consultation from external parties.

- Interoperability level:
  - Technical interoperability/Syntactical interoperability/ Semantic interoperability.
- Standards:
  - UDG Alliance is mainly exploiting IoT standards developed by various SDOs.
- Supporting organizations:
  - University and European SMEs.
- Domain:
  - UDG Alliance encompasses both consumer and industrial Internet.
  - It encompasses bot connectivity and application layers, with a cross domain positioning.
- Application area:
  - UDG Alliance is fully cross-domain, encompassing smart buildings, smart cities, smart agriculture, etc.
- Scope:
  - Integration/Interoperability knowledge area.
- IPR Policy Available:
  - Specific access rules defined by the Alliance.
- Specification Access:
  - Non-published specifications: freely accessible to members only; not accessible to non-members.

5.2.30 World Wide Web Consortium (W3C)

W3C is an international member-funded organization focusing on standards and guidelines for web technologies, including web browsers, web data and metadata, as well as horizontal activities on accessibility, internationalization, privacy and security. W3C specifications are implementable under a royalty free patent policy and are available as free downloads.

Web applications execute on cloud servers, and at the network edge in web browsers. W3C's standards activities for the IoT and Edge Computing include the Web of Things, Decentralized Identifiers, WebNN for local and federated AI, WASM for speeding up applications at the edge, RDF and Linked Data, and early work on Cognitive AI.

Web of Things

The Web of Things is an abstraction layer for sensors and actuators where applications interact with digital twins independently of the protocols and data formats used to communicate with the IoT devices. This is based upon using RDF to describe digital twins in terms of their affordances (properties, actions and events), their associated data models and semantics, and the security and communications metadata for use by client platforms to connect to the IoT devices.

W3C released standards for Thing Descriptions in JSON -LD and the Web of Things Architecture as W3C Recommendations in April 2020, along with informative reports on a scripting API and security and privacy guidelines. Related work is addressing binding templates and discovery. For more details, see: https://www.w3.org/WoT/.

The Web of Things is applicable across many sectors, e.g., smart buildings, smart homes, smart cities and manufacturing.

Web Neural Network API

This is a low-level API for artificial neural networks with hardware acceleration, and can be used to execute pre-trained models as well as for local and federated machine learning. The Web Neural Network API is designed for execution at the network edge and can be applied to a wide range of applications. For more details, see: https://www.w3.org/groups/wg/webmachinelearning

Web Assembly

Web Assembly (Wasm) is designed as a portable target for compilation of high-level languages, enabling deployment on the Web for client and server applications. Web Assembly aims to execute at native speed, taking advantage of common hardware capabilities, and its binaries are much smaller than JavaScript files. This makes them faster to download, faster to decode and execute. It has been used for a wide range of applications, and can be used outside of the Web browser, e.g., for server-less computing. Compilers are available for C/C++, C#, Rust, Go, Kotlin, Swift and other languages. For more details, see: https://www.w3.org/wasm/

RDF and Linked Data

RDF is W3C's framework for graph data and metadata, and important for the IoT in respect to semantic interoperability whereby providers and consumers can agree on the meaning of data and metadata. There is a suite of existing standards including the OWL ontology language, the SPARQL query language and SHACL, the RDF shape constraints language. RDF defines an abstract model that can be serialised in a variety of formats including XML, Turtle and JSON-LD. RDF supports URIs for graph nodes and link predicates. URIs are globally unique identifiers and as such useful for standardising vocabulary terms as a basis for semantic interoperability. RDF URIs can be dereferenceable as a means to obtain further information. The Linked Data Platform (LDP) defines a set of rules for HTTP operations on web resources, some based upon RDF as an architecture for read-write Linked Data on the Web.

Cognitive AI

Classical AI is based on symbolic representations, search algorithms, rule languages and logical deduction. The dependence on manual knowledge engineering imposes a scaling bottleneck. By contrast, deep learning with artificial neural networks derive their power from machine learning using huge data sets.

Deep learning is good at deep statistical correlations, but has difficulties with salience and generalising beyond the training data. There is increasing awareness of the potential for hybrid approaches that combine symbolic and sub-symbolic statistical techniques. Cognitive AI seeks inspiration from the human brain as the only example of general intelligence we currently have.

Cognitive AI is still at an early stage. The W3C Cognitive AI Community Group is working on mimicking human perception, cognition, feelings and action. Chunks are based upon work in the cognitive sciences on human memory and the idea of chunking information to make it easier to recall. The chunks and rules specification describes chunk graphs and rules. It can be implemented on edge computers as a basis for combining the IoT with local or remote cognition. Chunks offer a simple way to reconcile Property Graphs and Semantic Graphs, and includes a mapping to RDF. For more details, see: https://www.w3.org/community/cogai/

Web Machine Learning Working Group

W3C is also working on standards for accelerating performance of web applications in the browser through lower level access to hardware, e.g. graphics accelerators and hardware acceleration of artificial neural networks, where we held a workshop and are now in the process of launching a new Web AI working group see: https://www.w3.org/groups/wg/webmachinelearning.

W3C Decentralized Identifier Working Group

- Description:

  Decentralized identifiers (DIDs) are a new type of identifier that enables verifiable, decentralized digital identity. A DID refers to any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) as determined by the controller of the DID. In contrast to typical, federated identifiers, DIDs have been designed so that they may be decoupled from centralized registries, identity providers, and certificate authorities. Specifically, while other parties might be used to help enable the discovery of information related to a DID, the design enables the controller of a DID to prove control over it without requiring permission from any other party. DIDs are URIs that associate a DID subject with a DID document allowing trustable interactions associated with that subject.

  Each DID document can express cryptographic material, verification methods, or services, which provide a set of mechanisms enabling a DID controller to prove control of the DID. Services enable trusted interactions associated with the DID subject. A DID might provide the means to return the DID subject itself, if the DID subject is an information resource such as a data model.

  Decentralized identifiers v1.0 is a W3C Candidate Recommendation as of 27 June 2021, for more details, see https://www.w3.org/2019/did-wg/

  The mission of the W3C Decentralized Identifier Working Group is to standardize the DID URI scheme, the data model and syntax of DID Documents, which contain information related to DIDs that enable the aforementioned initial use cases, and the requirements for DID Method specifications.

  The W3C DID Working Group is closely allied with the groups and activities mentioned in the W3C introductions, such as:

  - Credential Community Group
  - The Web of Things
  - RDF and Linked data
  - Cognitive AI
  - Web Machine Learning Working Group

- Readiness:
  - Adoption:
    - Decentralized identifiers v1.0 is a W3C Candidate Recommendation as of 27 June 2021
  - Development status:
    - Decentralized identifiers v1.0 is a W3C Candidate Recommendation as of 27 June 2021
  - Compliance:
  - Openness:
    - Open access via GitHub
    - Ratification process (how the standard is being approved?):

- Interoperability level:
    - Syntactical interoperability (Yes)
    - Technical interoperability (Yes)
    - Semantic interoperability (Yes)
- Standards:
    - Decentralized Identifiers (DIDs) v1.0, Core architecture, data model, and representations (W3C Candidate Recommendation, May2021. Recommendation anticipated ca. September 2021).
- Supporting organizations:
- Domain:
    - IoT and edge computing
- Application area:
- IPR Policy Available:
    - W3C specifications are implementable under a royalty free patent policy and are available as free downloads.
- Specification Access:
    - Free download

5.2.31 WWRF (Wireless World Research Forum)

- Description:

  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. The supported features are:

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

- Readiness:

  1. Adoption:
     - 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
     - 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:
  - Standards are not developed by WWRF, so no interoperability level applies.
- Standards:
  - 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
  - Nokia, Huawei and China Mobile are sponsors, other members include: Qualcomm, Fujitsu, Bell Canada, Sagem, HP, NEC, Ericsson, Intel, LG, DoCoMo.
- Domain:
  - WWRF covers all these areas, so a position close to the centre is appropriate.
- Application area:
  - Horizontal/Telecommunication.
- Scope:
  - Communication and Connectivity knowledge area.
  - Applications knowledge area.
  - Infrastructure knowledge area.

- IPR Policy Available:
    - 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:
    - 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/
Civil Infrastructure Platform (CIP)	https://www.cip-project.org/
Contiki	http://www.contiki-os.org/
EclipseIoT	http://iot.eclipse.org/
Eclipse IoT-Testware	https://projects.eclipse.org/projects/technology.iottestware
EdgeX Foundry	https://www.edgexfoundry.org/
FIT IoT Lab (Testbed)	https://www.iot-lab.info/
Fi-ware	www.fiware.org
FlockLab (Testbed)	https://gitlab.ethz.ch/tec/public/flocklab/wiki
IoTivity	https://www.iotivity.org/
IoT6	http://iot6.eu/
InfluxDB	https://influxdb.com/
LinuxIoTDM	https://wiki.opendaylight.org/view/IoTDM:Main
Matter	https://buildwithmatter.com/
mozaiq	http://www.mozaiq-operations.com/about-us/
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
The things Network	https://www.thethingsnetwork.org/
ThingSpeak	https://thingspeak.com/
Tiny OS	http://www.tinyos.net/
universAAL	http://www.universaal.info/
Warp 10 Platform	http://www.warp10.io

5.3.1 Matter

- Description:

  This industry unifying standard is a promise of reliable, secure connectivity—a seal of approval that devices will work seamlessly together, today and tomorrow. Matter (https://buildwithmatter.com/) is creating more connections between more objects, simplifying development for manufacturers and increasing compatibility for consumers. This collaborative breakthrough is built on proven technologies and guided by the Connectivity Standards Alliance (formerly Zigbee Alliance), whose members come together from across industries to transform the future of connectivity.

  Matter is built around a shared belief that Smart home devices should be secure, reliable, and seamless to use. By building upon Internet Protocol (IP), Matter will enable communication across smart home devices, mobile app and cloud services and to define a specific set of IP-based networking technologies for device certification.

- Readiness:

  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

  5. Licensing:

  - Apache License version 2.0

  6. Portability:

  ▪ Platform independent.

- Interoperability level:

  - Organizational interoperability

- Standards:

  - Matter, based on Internet Protocol (IP) and developed by the Connectivity Standards Alliance (formerly Zigbee Alliance)

- Supporting organizations:

  - Amazon, Apple, Google, Zigbee Alliance and others.

- Domain:

  - Matter is focused on Services and Applications for Consumer Market.

- Application area:

  - Matter makes it easier for device manufacturers to build devices that are compatible with smart home and voice services such as Amazon's Alexa, Apple's Siri, Google's Assistant, and others. The first specification release of the Matter protocol will run on Wi-Fi and Thread network layers and will use Bluetooth Low Energy for commissioning.

- IPR Policy Available:

  - https://zigbeealliance.org/about/governing-documents-ipr/

- Specification Access:

  - The Project's design and technical processes are intended to be open and transparent to the general public, including to Work Group non-members wherever possible. The availability of a GitHub repository and its source code under an Apache v2 license is an important and demonstrable step to achieving this commitment.

  - https://github.com/project-chip/connectedhomeip

5.3.2 Civil Infrastructure Platform (CIP)

- Description:

  The Civil Infrastructure Platform ("CIP") is a collaborative, open source project hosted by the Linux Foundation. The CIP project is focused on establishing an open source "base layer" of industrial grade software to enable the use and implementation of software building blocks in civil infrastructure projects. Currently, civil infrastructure systems are built from the ground up, with little re- use of existing software building blocks.

  The CIP project intends to create reusable building blocks that meet the safety, reliability and other requirements of industrial and civil infrastructure. By establishing this 'base layer', CIP aims to:

  - Speed up implementation of civil infrastructure systems.
  - Build upon existing open source foundations and expertise without reinventing non-domain specific technology.
  - Establish (de facto) standards by providing a base layer reference implementation.
  - Contribute to and influence upstream projects regarding industrial needs.
  - Motivate suppliers to actively support these platform / provide an implementation.
  - Promote long term stability and maintainability of the base layer of code.
- Readiness:
  1. Community:
     - Multiple organizations (have to be Linux Foundation member).
  2. Commitment:
     - Formally appointed committers from organizations.
  3. Road Map:
  4. Alignment of ongoing Standards:
     - Not applicable.
  5. Licensing:
     - GPL 2.0 (contributions to the Linux Kernel), Apache V2.0 (contributions not involving the Linux Kernel).
  6. Portability:
     - Only one target platform; CIP is the platform.
- Interoperability level:
  - Technical.
- Standards:
  - Linux based.
- Member organizations:
  - Hitachi, Siemens, Toshiba, Codethink, Plat'Home.
- Domain:
  - Industrial, Service&App (SW platform).
- Application area:
  - Any technical systems responsible for supervision, control, and management of infrastructure supporting human activities, including, for example, electric power generation and energy distribution, oil and gas, water and wastewater, healthcare, communications, transportation, and community management. These systems deliver essential services, provide shelter, and support social interactions and economic development. They are society's lifelines.
- Scope:
  - Infrastructure knowledge area (SW Platform, Operating System).
- IPR Policy:
- Specification Access:
  - Open Source

5.3.3 Eclipse IoT-Testware

- Description:
  It is the aim of the project to supply a rich set of TTCN-3 test suites and test cases for IoT technologies to enable developers in setting up a comprehensive test environment of their own, if needed from the beginning of a project. TTCN-3 has been defined and standardized by the European Telecommunication Standards Institute in ETSI ES 201 873 and related extension packages. It is implemented and supported by the Eclipse Titan project.
- Readiness:
  1. Community
     - Multiple organizations.
  2. Commitment
     - Multiple volunteer committers.
  3. Road map:
     - Frequent but non planned releases (small extension).
     - Planned releases (synchronization with standards).
  4. Alignment of ongoing Standards:
     - Not aligned with SDO standards (in case of extended scope).
     - OSS output is aligned with SDO specifications (in case of updates).
  5. Licensing:
     - Eclipse Public License 1.0
  6. Portability:
     - Platform independent.
- Interoperability level:
  - Technical interoperability: addresses various IoT protocols and platforms (e.g. CoAP, MQTT, OPC-UA, LwM2M).
  - Syntactical interoperability: may be subject of future test suites but depend on developer's resources and decisions.
- Standards:
  Various SDO and consortia standards and protocols related to the test suites will be used and supported; sources will include IETF (CoAP), OASIS (MQTT), OPC Foundation (OPC-UA), OMA (LwM2M) etc.
- Supporting organizations:
  - Fraunhofer FOKUS
  - relayr GmbH
  - Ericsson
  - Spirent Communication
  - Sintesio Foundation
  - EasyGlobalMarket (EGM)
- Domain:
- Initiative is related to multiple market domains (consumer/industrial internet) and the technical domain (connectivity, service and applications), i.e. in Figure 3 close to ETSI's positions in Figure 1.
- Application area:
  - Initiative is focusing on integrated/complete IoT solutions, i.e. horizontal industry, and do not exclude a particular vertical industry.

- Scope:
  - Communication and Connectivity knowledge area:
    - It covers testing of communication protocol layers
  - Integration/Interoperability knowledge area:
    - It covers mainly testing of common IoT features required to provide integration and interoperability.
  - Applications knowledge area:
    - Applications testing may be included if specific applications has been identified as of general interest.
  - Infrastructure knowledge area:
    - It covers aspects related to testing during design, deployment, and operation.
  - IoT Architecture knowledge area:
    - It may support integrated/complete IoT testing solutions, including aspects on performance, but this is subject of the developer's resources and decisions.
  - Devices and sensor technology knowledge area:
    - It do not exclude device/sensor lifecycles, operating systems, platforms, configuration management, sensor/actuators virtualization etc., but this is subject of the developer's resources and decisions.
  - Security and Privacy knowledge area:
    - It will include fuzzing tests.
- IPR Policy Available:
  Eclipse Public License 1.0, https://www.eclipse.org/org/documents/epl-v10.php
- Specification Access: https://projects.eclipse.org/projects/technology.iottestware/developer

5.3.4 IoTivity

- Description:

  IoTivity is an Open Source Project sponsored by the Open Connectivity Foundation (OCF) / 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 OCF / 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.

  OCF / 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:

  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 – OFC / OIC.
  5. Licensing:
     - Apache License version 2.0.
  6. Portability:
     - Multiple platforms are developed by project.

- Interoperability level:
  - Organisational interoperability. Note work is ongoing to interoperate through the OneM2M platform as well as across the OCF / OIC ecosystem.
- Standards:
- OCF / OIC.
- Supporting organizations
- OCF / OIC.
- Domain:
  - Multiple domains – initial release has a consumer focus with a mix of connectivity and services.
- Application area:
  - Different specifications cover different areas. The initial focus is on Smart Home.

- Scope:
    - 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:
    - FRAND – Free licensing.
- Specification Access:
    - Code open on IoTivity web site – free to access for all - https://www.iotivity.org/.

5.3.5 IoT6

- Description:

  IoT6 is an IPv6-based protocol pile for the IoT developed by the European research project IoT6. It enables multiple IoT systems integration, including with building automation, tags, mobilephones, cloud application (Software as a Service), sensor networks, etc. It has been designed to enable native IPv6 integration of heterogeneous IoT devices with IPv6 security enablers. It encompasses the various OSI layers, up to the application layer.

- Readiness:

  1. Adoption
     - Reference implementations; used by several European research projects, as well as in IoT deployment across Europe and Asia.

  2. Development Status
     - Approved with planned revisions.
     - Global standardization at ITU started

  3. Compliance
     - With various IoT standards, including UDG for non-IP standards interoperability.

  4. Openness
     - Open; in process of global standardization through the ITU.

  5. Ratification process
     - Through consensus building, tests and interoperability validation
     - Currently following ITU process.

- Interoperability level:
  - Technical interoperability/Syntactical interoperability/ Semantic interoperability.
- Standards:
  - IoT6 is leveraging on various IoT standards developed by various SDOs and specific developments.
- Supporting organizations
  - Several European and Asian universities, industries and SMEs.
- Domain:
  - IoT6 encompasses both consumer and industrial Internet.
  - It encompasses bot connectivity and application layers, with a cross domain positioning.
- Application area:
  - IoT6 is fully cross-domain, encompassing smart buildings, smart cities, smart agriculture, etc.
- Scope:
- IPR Policy Available:
  - Part of the specifications are open, specific access rules are defined by IoT6.
- Specification Access:
  - Partially published.
  - New version to be accessible to IoT6 and ITU members.

5.3.6 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:

  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:
  - 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.
- IPR Policy Available:
  - Eclipse Public License (ou EPL).
- Specification Access:
  - http://eclipse.org/om2m.

5.3.7 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.

  The supported features are:

  - 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:

  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:
  - 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:
  - Supported standards: CoAP, Zigbee, enOcean, KNX, NFC, BLE, MQTT, XMPP, OMA NGSI, OMA LWM2M, OneM2M, CDMI.
  - Leveraging the OSGi standard.

- Supporting organizations
  - CEA is the main organization + several industrial and academic partners providing their support.

- Domain:
    - sensiNact is a platform for managing IoT services & applications. It is domain agnostic and can be applied to consumer or industrial business.
- Application area:
    - 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:
        - Communication and Connectivity knowledge area:
            - sensiNact provides protocol bridges for various communication protocols (Zigbee, KNX, enocean, MQTT, XMPP, CoAP, etc.).
        - Integration/Interoperability knowledge area.
        - Applications knowledge area:
            - sensiNact provides SDK and tool for IoT application development, deployment and run-time management.
        - Infrastructure knowledge area.
        - IoT Architecture knowledge area:
            - 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:
            - sensiNact is agnostic to device and sensor technologies.
        - Security and Privacy knowledge area:
            - Provides token based authentication and profile based authorization.
- IPR Policy Available:
    - Apache Software License 2.0.
- Specification Access:
    - First public information at http://open-platforms.eu/library/butler-smart-gateway/. Github repository under construction.

5.3.8 Sofia2

- Description:

  Sofia2 is a horizontal IoT Platform with Big Data capacities created from the Artemis European project SOFIA (SMART OBJECTS FOR INTELLIGENT APPLICATIONS). SOFIA is a platform for semantic interoperability developed for 3 years by 18 partners and 4 countries in Europe. SOFIA proved its effectiveness in over 7 pilots related to contexts such as Smart City, Smart Spaces.

  After the end of the SOFIA project we decide to benefit from the acquired knowledge of the project and order to create an IoT Platform with a business approach: Sofia2. Sofia2 can be described as a middleware + repository capable of processing thousands event per second, with Big data storage capabilities with integrated rules, interfaces, multi protocols and Multilanguage and all this is operable from a web console.

  Sofia2 has application to fields as Smart Cities, Energy, Health, Home, Transportation, Finance, Security, Insurance, Banking, Manufacturing, Industry, Office. Sofia2 mainly features are:

    - Integrated Platform (not acoplated) in which all concepts (such as security, modelling, rules, queries, Big Data, CEP, APIs) function in an integrated way.
    - Centralized console (and REST API) to configure and operate the entire platform.
    - Integrated and comprehensive security.
    - Customizable and extensible by the Organization by plugins.
    - Multi-device approach: with APIS for major languages (e.g., Java, Javascript, Android, iOS, .NET, Python, Node.js, Arduino) in addition to an universal REST API.
    - Multiprotocol: supporting bi-directional communication protocols such as REST, MQTT, JMS, WebSockets, WebServices.
    - Big Data capabilities integrated: supported on Hadoop.
    - Horizontal scalability of the entire platform, this allows you to start with a limited deployment and go to grow as needs.
    - Cloud and On Premise Deployment supported: Sofia2 runs on Public Clouds as Azure, Google CE, Amazon AWS as PaaS.
    - Open Source Version and commercial supported Version.
    - Supported in standards and market technologies.
    - Semantic view.
    - Technical add-on modules as API Manager, dashboards, reports, nalytics, CEP, rules.

- Readiness:

  1. Community: main contributor Indra + contributions of different partners around the world.
     - Commitment: mostly one committer + committers of different partners + volunteers from around the world about the community.
  2. Roadmap: planned releases (each 2 months) and a Formal roadmap.
  3. Alignment of ongoing standards: support for various IoT Standards, active participation on standards (such as OSGi, Zigbee).
  4. Licensing: dual. OSS license is AGPL, Commercial License too.
  5. Portability: Platform independent. (Built on Java mainly).

- Interoperability level:

    - Syntactical interoperability:
        - Defines ontology (entity) in JSON format by JSON Schema.
        - Platform concepts modelled from Web console or by REST API (e.g., security, rules, CEP rules, dashboards, reports).

- Technical interoperability:
    - Support of various protocols and platforms IoT (e.g., MQTT, NGSI, CoAP, REST, JMS, WebSockets).
- Semantic Interoperability:
    - Ontology Model supports standards as JSON-LD, OGC SensorThings, AMON.
- Organizational Interoperability:
    - Support of various enterprise protocols as WebServices, REST, JMS, AMQP.
    - Support of customized security, adaptable for enterprise needs.

- Standards:
    - Supported standards: REST, JSON, MQTT, WebSockets, Web Services , NGSI, Java.
    - On device part support BLE, Zigbee, Zwave, 6LowPan, MQTT, OSGi.
    - Pluggable architecture with the capability of including new protocols when protocols get standardized.
- Supporting organizations:
    - Indra as the main organization and as well different companies, universities, entrepreneurs creating and evolving modules.
- Domain:
    - Horizontal IoT Platform with Big Data and Analytics Capabilities for developing Vertical Solutions. Domain agnostic, applicable to enterprise business mainly.
    - On the quadrant Sofia2 (horizontal axis on Industrial Internet Market although Sofia2 is also used on Consumer Market, vertical Axis as Core for Service&Apps).
- Application area:
    - As Horizontal IoT Platform can be used in any industry: Smart Cities, Energy, Health, Home, Transportation, Finance, Security, Insurance, Banking, Manufacturing, Industry, Office.
    - Sofia2 has already deployments on Smart Cities, Smart Energy, Smart Home, Smart Health, Smart Transportation, Smart Banking.
    - Sofia2 is focusing on the creation of complete IoT Solutions working as the core of these solutions.
- Scope:
    - Communication and Connectivity knowledge area:
        - bridges for various communication protocols: e.g., MQTT, HTTP, REST, TCP, CoAP, JMS, Zigbee, BLE.
    - Integration/Interoperability knowledge area:
        - any Thing can connect to the platform by the Multilanguage APIS. In addition it supports standards connectors on REST, MQTT, WebServices and WebSockets, web modeling of information from devices. Bi-directional communication.
    - Application Knowledge area:
        - Development tools: SDK Linux/Windows/Mac. APIS on different languages as Java, Javascript, C, C++, Python, Arduino, Android, iOS, .NET.
        - Deployment and management: Centralized Web Console + APIS REST supporting the full cycle of development. Deployment in all Public Cloud (images on Azure, Google CE and Amazon EWS) as a country. Deployment On Premise as Java deployables on any AppServer (e.g., Weblogic, WebSphere, Tomcat, Jboss).
        - Other modules: API Manager, CEP, Rules.

        - Analytics Tools: Dashboards, Reports, Rules on Java, R and Python. SQL Query Integrated with BA Tools as Microsoft BA.
        - Application Domain Specifics: ontologies on different domains (Smart Cities, Smart Energy, Smart Home, Smart Health). Verticalizations of the platform.
    - Infrastructure knowledge area:
        - Deployment on any public Cloud as PaaS, support models Fog Computing, Big Data approach.
    - IoT Architecture knowledge area:
        - Built on Java and Spring technologies, support modules on Java, Python and R.
    - Devices and sensor technology knowledge area:
        - Agnostic to device and sensor technologies. Provides Multilanguage APIS to simplify development. Offers frameworks for simplified developing on devices/Intel ARM providing version management, development on protocols (such as BLE, Zigbee, 6LowPan, Zwave).
    - Security and Privacy knowledge area:
        - Security integrated on the core. Supports authentication and authorization based on user/password, tokens, electronic certificates, Security pluggable can be personalized and extended.
- IPR Policy Available:
    - Open Source Version: Platform on AGPL v3 (GNU Affero General Public License). APIS on Apache 2.0.
    - Commercial Version: different models.
- Specification Access:
    - On the url http://sofia2.com any person can get access to different documentation of Sofia2, from specifications to user guides.
    - On the url http://sofia2.com/console/login any person can register and get access to a free unlimited Cloud version of the Platform (Sofia2 CloudLab).
    - On the url http://sofia2.org people can ask for access to OOS version of Sofia2, Indra verifies he identity of the person and allow the access to the software.
    - On the url https://github.com/Sofia2 SDO any person can download Sofia2 APIS (Interfaces for connecting with the Platform in different languages).

5.3.9 UniversAAL IoT

- Description:

  Objective: Overcome the intensified overhead of integrating the complex systems of systems of the digital era by providing open specifications for semantic interoperability to enable cross-domain constellations while minimizing integration and deployment costs; such specifications to be implemented by open source and free software resulting in global standards and commoditised infrastructure solutions and tools, altogether providing an open service platform around which an open and self-organizing ecosystem may emerge.

  Features:

  (1) A Framework for connectivity, communication and semantic interoperation between otherwise disparate Products, Services and Devices,

  (2) this way achieving interoperability across domains, vendors, devices, locations, and deployment strategies,

  (3) with support for the implementation of the Sensing-Reasoning-Acting pattern,

  (4) utilizing the cumulative potential of the sum total of capabilities within open distributed systems of systems,

  (5) as well as different deployment strategies (although the concept definitions back in 2007 were based on the paradigm of Edge Computing, it supports multi-tenant deployments as well as pure Could-based deployments)

  Unique characteristics:

  (1) implementation of semantic interoperability for SoA at the level of communication protocols that eliminates the need for domain-specific APIs by reducing syntactical dependencies to one single brokerage API,

  (2) Support for context-awareness with ontology-based data sharing, intuitive model with no dependency on domain-specific ontologies, distributed push & pull mechanisms, an associated RDF database supplemented with situation reasoning, extensible with further reasoners, and some good ontologies, especially the "physical world" ontology, and

  (3) Support for user interaction in smart environments (see IEC PAS 62883) based on the notion of "interaction channels" (ICs) and UI Handlers as IC managers, with situation-aware selection of UI Handlers for handling applications' UI requests, automatically making the applications multimodal, loss-less dynamic change of IC (e.g., automatic "follow me" or automatic switching between private and public ICs), and location-based notion of "sessions" with users

- Readiness:

  Certain parts of the platform have reached the technology readiness level TRL-9 with actual proof in operational environment running for 1.5 years seven days a week, 24 hours a day; some other parts of universAAL IoT completed the prototype demonstration phase (TRL-7). It is also clearer now what should be the next priorities in the maintenance and further development of universAAL IoT.

  1. Community: Multiple organizations from the European public sector

  The "Formal consortium" called "The universAAL IoT Coalition (uIC)" has been created 2018 as an open, non-profit, international association based in Brussels, but is not really active yet.

  2. Commitment: Multiple volunteer committers

  3. Road map: since 2018 only sporadic releases (due to the good level of maturity in real-life deployments on one side, and lack of dedicated budget on the other side)

  4. Alignment of ongoing Standards: Not directly aligned with SDO standards but relies mostly on the Semantic Web specifications RDF, OWL and SPARQL

  5. Licensing: Apache Software License 2.0

  6. Portability: supported runtime environments are Java OSGi and Java Android with local Java APIs, but provides also a REST API for remote access from different heterogeneous runtime environments; communication between different runtime environments is based on plain text, with Turtle syntax (alternatively JSON-LD), so that there is no obstacle in supporting several heterogeneous runtime environments, by porting the API to such other runtime environments.

- Interoperability level:

  Syntactical interoperability: Turtle syntax/ JSON-LD based on RDF standard specifications

  Semantic interoperability: substitutes domain-specific APIs (syntactical dependencies between interoperable modules) by pluggable shared / compatible domain models (ontologies)

  Organisational interoperability: facilitates the creation of open distributed multi-vendor systems made from heterogeneous subsystems based on shared / compatible ontologies; not only data and information, but also functionality can be shared without any technical or syntactical dependency between the heterogeneous systems of different vendors

- Standards:

  several existing standards are being used and supported; the main set of standards used is the set produced by the Semantic Web community of the W3C. From universAAL IoT, there are several specifications that have the potential to become global standards, one of which has reached the status of an IEC PAS (Publically Available Specification); the community is looking for the right context to place its proven specifications as standardization candidates.

- Supporting organizations:

  www.igd.fraunhofer.de, www.sabien.upv.es, www.lst.tfo.upm.es, and www.isti.cnr.it

- Domain:

  equally relevant for both B2B and B2C, but the API is more relevant for "Service & App" rather than "Connectivity" (because for Connectivity, it is only providing a framework for bridging different connectivity solutions to the universAAL IoT ecosystem based on semantic communication and compatibility)

- Application area:

  universAAL IoT provides a horizontal service and application integration layer across all verticals so that it can be used for integrating arbitrary open distributed systems of systems but so far, all real-life deployments of universAAL IoT are related to smart living environments.

- IPR Policy Available:

  universAAL IoT is provided under the Apache Software License 2.0, which explicitly guarantees that there are no hidden patents and any possibly existing patent is included in the royalty-free distribution with unlimited usage rights, including commercialization by third parties.

- Specification Access:

  - all publicly available under https://github.com/universAAL/
    Technical overview: universaal.info/site_files/6325/upload_files/universAAL-IoT_technical-overview.pdf

5.3.10 Warp10 from Cityzen Data

- Description:

  Warp10 provides:

  - Data management and analytics technology for sensors data, machine data, IoT Data;
  - Open Source Distribution (http://www.warp10.io);
  - Hadoop framework Database;
  - Major and specific key value :
    - It stores and manipulates data defined by time and location (Geo Time Series™);
    - It performs generic and advanced 600 functions and IoT generic algorithms which are adaptable to any business (energy, transport, home and cities, monitoring, security …);
    - It proposes a value added language to go faster including development and processing;
    - It ingests real-time data from 100K to 1500K Datapoint/sec/core;
    - It provides predictive analysis in a generic IoT perspective;
    - It provides security features by 1) encrypting all geo time metadata, 2) managing rights by allowing dynamic tokens, 3) encapsulating all functions, algorithms and tools developed by clients or third parties in its own language;
    - It proposes a clear distinction between technical data management and analytics on one side, and data governance on the other side.

  13.

- Readiness:

  1. Community:
     - Technology developed by Cityzen Data (www.cityzendata.com).
     - Open Source distribution since Jan 2016.
     - Community: https://groups.google.com/forum/#!forum/warp10-users .

  2. Commitment:
     - Opened to any user / developer.

  3. Road map:
     - Frequent but non planned releases (release when ready).

  4. Alignment of ongoing Standards:
     - Web standards (W3C).

  5. Licensing:
     - Apache 2.0.

  6. Portability:
     - One platform is proposed by Cityzen Data.
     - Warp10 can be implement on any business IoT platform (Time series oriented).

- Interoperability level:
  - Technical interoperability: Universal Geo Times Series™ data format.
  - The technology has no direct concern with the telecommunications standards. Interfaces are based on HTTP protocols family.

- Standards:
  - The technology has no direct concern with the telecommunications standards. Interfaces are based on HTTP protocols family.

- Supporting organizations :
    - Cityzen Data is member of the BDVA (Europpe Big Data Value Association).
- Domain:
    - B2B.

      Applications level. However, it is the generic and technical side of applications level. Not the business application or the user application level.
- Application area:
    - Totaly generic for IoT Data.
    - Warp10 allows to build up a real data infrastructure.
    - Scope:
        - Applications knowledge area:
        - IPR Policy Available:
            - Free.
        - Specification Access:
    - http://www.warp10.io

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 WLAN (Wireless Local Access Network) and WPAN (Wireless Personal Area Network) technologies can also be enabled to support a wider coverage e.g., Neighbourhood Area deployments. In case of wider coverage necessity, 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.

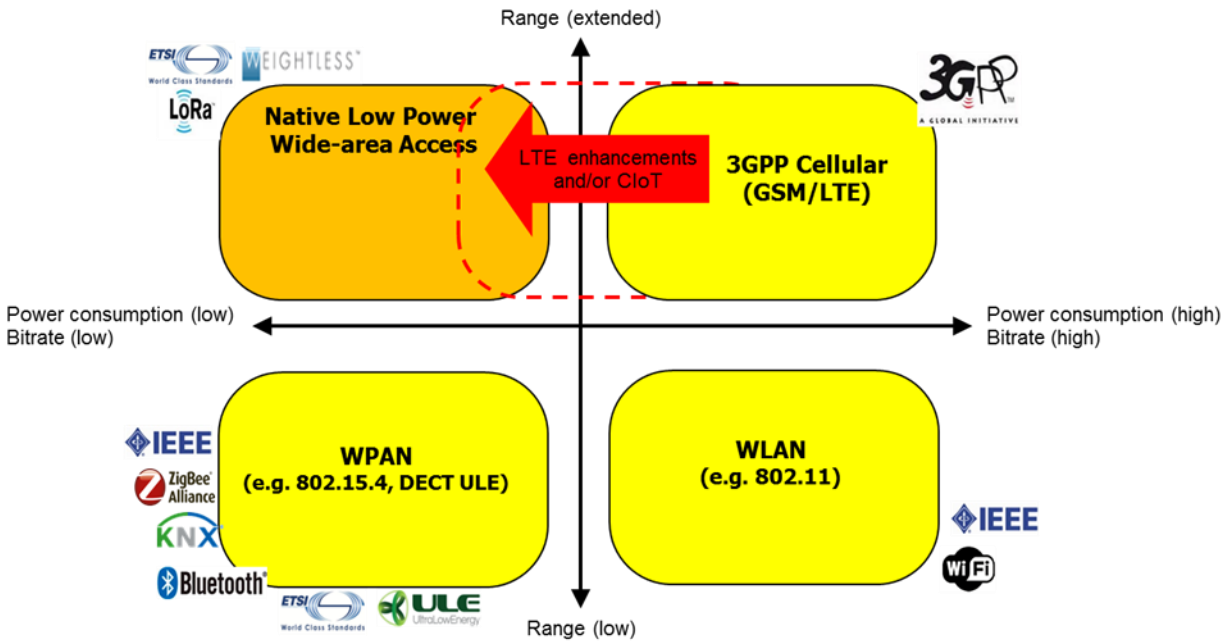


Figure 6: Wireless Connectivity Trends

References

[ETSI-position] "ETSI White Paper No. 3: Achieving Technical Interoperability - the ETSI Approach", ETSI White paper

[IERC-position] "Internet of Things, IoT Semantic Interoperability: Research Challenges, Best Practices, Recommendations and Next Steps"

Editor and Contributors

The document was written by several participants of the AIOTI WG Standardisation.

Editor:

- Georgios Karagiannis, Huawei

Reviewer:

- Damir Filipovic, AIOTI Secretary General

Authors:

Name	Company/Organisation
Tom de Block	Navigio
David Boswarthick	ETSI
Bruno Chatras	Orange
Marco Carugi	Huawei
Aitor Corchero Rodriguez	Eurecat
Omar Elloumi	Nokia
Lindsay Frost	NEC
Luis Miguel Gracia	Indra
Patrick Guillemin	ETSI
Sascha Hackel	Fraunhofer Fokus
Juergen Heiles	Siemens
Karen Hughes	oneM2M
Georgios Karagiannis	Huawei
Thomas Klein	IBM
Sylvain KUBLER	University of Luxembourg
Zbigniew Kopertowski	Orange
Antonio Kung	Trialog
Antonis Litke	Institute of Communication and Computer Systems
Andrea Lorelli	ETSI
Patricia Martigne	Orange
George Suciu	BEIA Consult
Jussi Numminen	Wirepas

Ranga Rao Venkatesha Prasad	Delft University of Technology
Friedhelm Rodermund	Vodafone
Maria Rossetti	MADE s.c.a r.l.
Mohammad-Reza Tazari	Fraunhofer IGD
Axel Rennoch	Fraunhofer Fokus
Erwin Schoitsch	Austrian Institute of Technology (AIT), Austria
Martin Serrano	National University of Ireland Galway
Ovidiu Vermesan	SINTEF
Alexander Vey	IBM
Ricardo Vittorino	Ubiwhere Lda
Sébastien Ziegler	Mandat International

Acknowledgements

About AIOTI

AIOTI is the multi-stakeholder platform for stimulating IoT and Edge Computing Innovation in Europe, bringing together small and large companies, academia, policy makers and end-users and representatives of society in an end-to-end approach. We work with partners in a global context. We strive to leverage, share and promote best practices in the IoT and Edge Computing ecosystems, be a one-stop point of information on all relevant aspects of IoT Innovation to its members while proactively addressing key issues and roadblocks for economic growth, acceptance and adoption of IoT and Edge Computing Innovation in society. AIOTI's contribution goes beyond technology and addresses horizontal elements across application domains, such as matchmaking and stimulating cooperation in IoT and Edge Computing ecosystems, creating joint research roadmaps, driving convergence of standards and interoperability and defining policies.