



AIOTI

ALLIANCE FOR INTERNET OF THINGS INNOVATION

Core values of AIOTI WG03

Patrick.guillemine@etsi.org – AIOTI www.aioti.org WG03 Chairman

georgios.karagiannis@huawei.com – AIOTI WG03 Co-Chairman

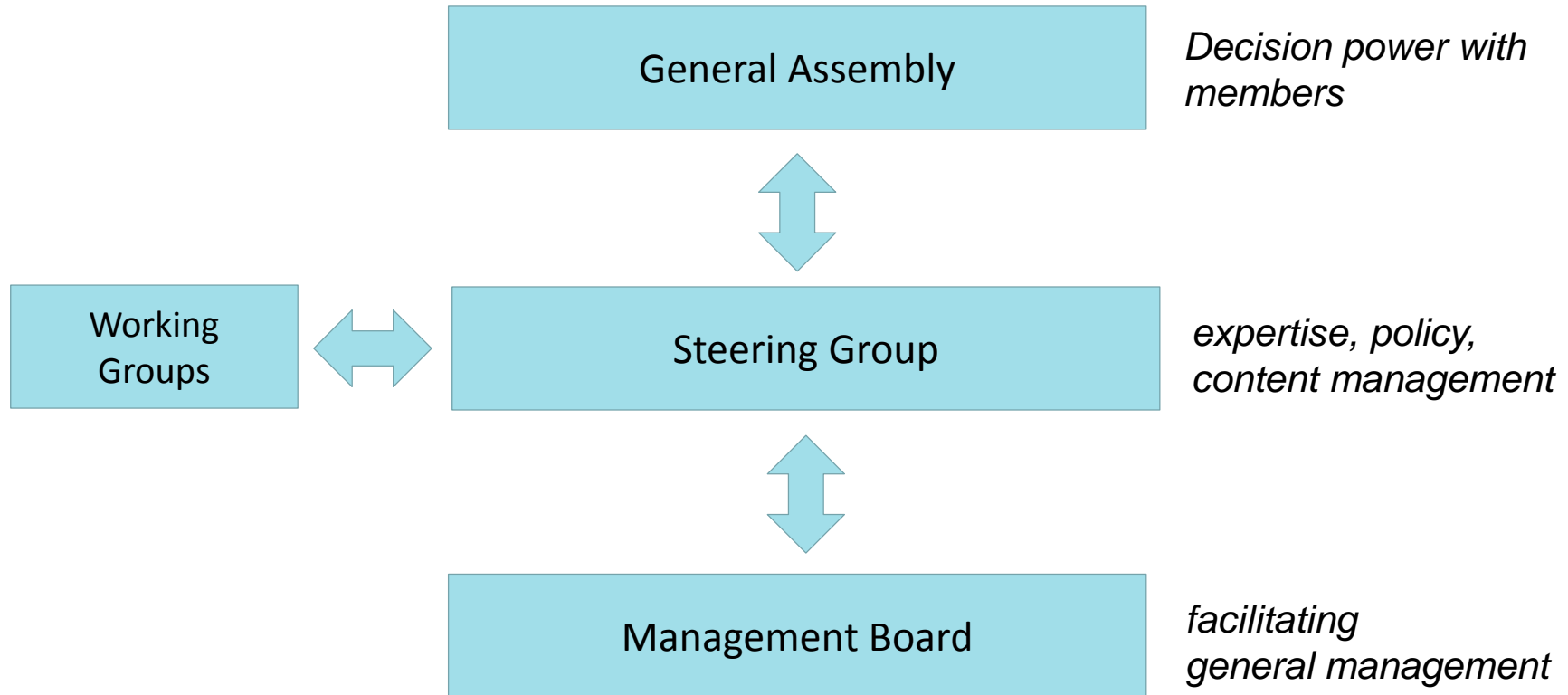
AIOTI - The Basis

- ❖ Create and master sustainable innovative European IoT ecosystems in the global context to address the challenges of IoT technology, applications and deployment including standardisation, interoperability and policy issues, in order to accelerate sustainable economic development and growth in the new emerging European and global digital markets
- ❖ Strengthen the integration across the digital value chain and foster coordination across different public funded industrial initiatives and support the acceleration of IoT deployment in a Digital Single Market context
- ❖ Promote global cooperation and collaboration in the area of IoT
- ❖ Mapping and bridging global, EU and Members States' IoT innovation activities



September 2016: AIOTI established as a legal Association

governance structure



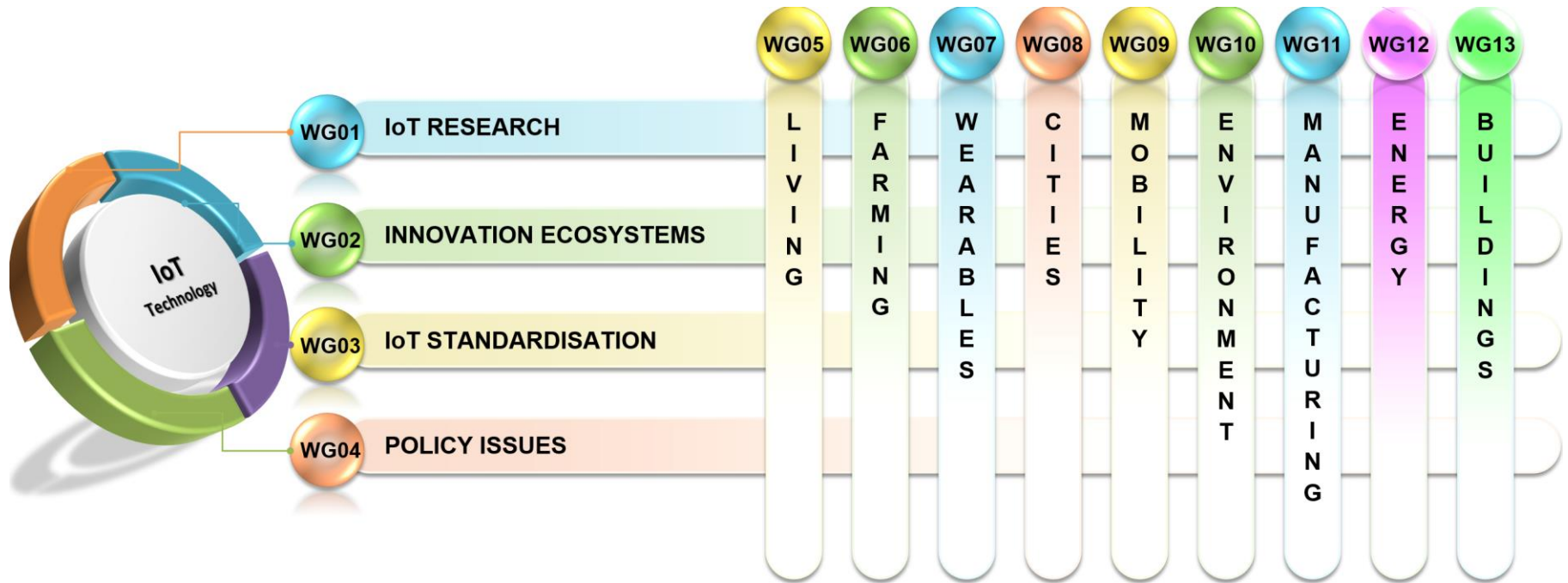
Note: every member is active in at least one Working Group



AIOTI

ALLIANCE FOR INTERNET OF THINGS INNOVATION

AIOTI WG Structure



AIOTI WG03

- ❖ Identifies and, where appropriate, makes recommendations to address existing IoT standards, analyses gaps in standardisation, and develops strategies and use cases aiming for (1) consolidation of architectural frameworks, reference architectures, and architectural styles in the IoT space, (2) (semantic) interoperability, (3) security by design support and (4) personal data & personal data protection to the various categories of stakeholders in the IoT space

- ❖ IoT Landscape / georgios.karagiannis@huawei.com
 - IoT Landscape maintenance is key to keep the liaisons alive and maintain dialogue on how to foster collaboration to improve interoperability & security
 - IoT-EPI IoT Platforms analysis improvement / H2020 UNIFY-IoT Ph. Moretto (ETSI STF)
 - Gap Analysis and recommendations / EC funded STF 505 E Darmois (ETSI STF)
 - Cooperation with SDOs/Alliances to foster co-creation and interworking (Patrick Guillemin)

- ❖ HLA / High Level Architecture / omar.elloumi@nokia.com
 - IoT Reference Architecture and its mapping with existing IoT Reference Architectures
 - IoT identification juergen.heiles@siemens.com ; henri.barthel@gs1.org

- ❖ IoT Semantic Interoperability Paul.Murdock@landisgyr.com
 - Important topic of the moment that created a great international collaboration

- ❖ IoT Privacy (with WG04) vanderwees@arthurslegal.com
 - IoT Platform, experimentation, LSPs need concrete standard framework & references to enable "IoT Trust" and IoT "Privacy by design"

- ❖ IoT Security (with WG04) vanderwees@arthurslegal.com,
jacques.kruse-brandao@nxp.com, harm.arendshorst@nl.verizon.com
 - IoT Security Architecture for Trusted IoT Devices; Baseline Requirements for Security & Privacy up to segment requirements; experimentation, LSPs need concrete standard framework & references to enable "IoT Trust" based on IoT "Security by design"



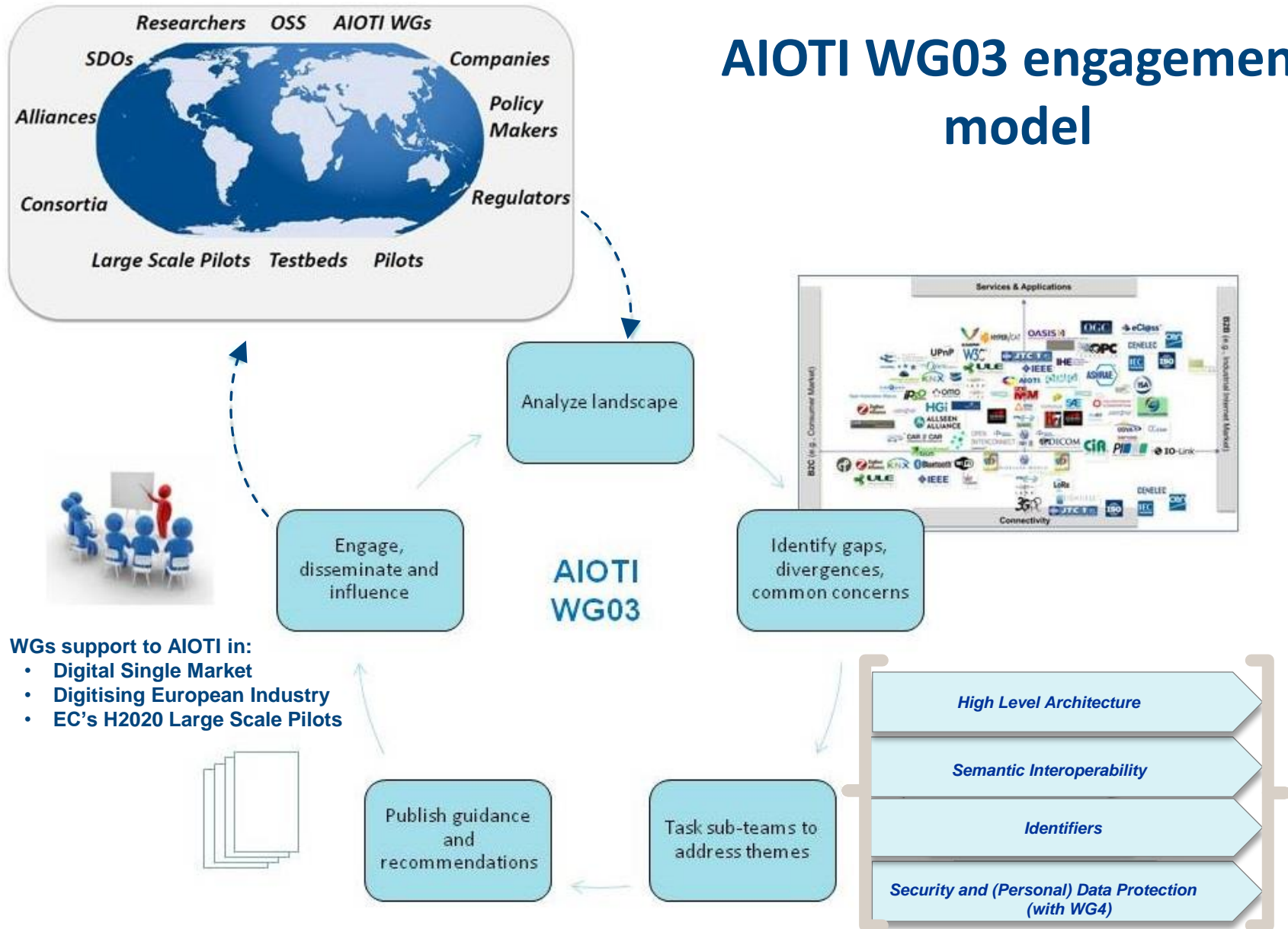
WG 03 IoT Landscape

Roadmaps: 2016 + 2017

- **Objective 1:** Identifying the gaps of emerging IoT standards and practices (ongoing)
- **Objective 2:** Report on the discussions with SDO/Alliance/OSS initiatives to foster co-creation and interworking, realise economies of scale and scope, mitigate fragmentation and contribute to solving the gaps on emerging IoT standards and practices (ongoing)
- **Objective 3:** Report on the cooperation and participation of vertical and horizontal industry, academia and research stakeholders into the IoT landscape activities (ongoing)
- **Objective 4:** Stepwise updating the IoT landscapes and elaborating in more depth the IoT knowledge areas (ongoing; new version by end of December 2016)
- **Objective 5:** Report on IoT-EPI IoT Platforms analysis improvement / H2020 UNIFY-IoT (ongoing)
- **Objective 6:** Cooperation with other AIOTI WGs on providing recommendations that (ongoing):
 - address inter application/domain interoperability issues
 - provides recommendations on using standard-based solutions for the deployment of IoT solutions
- **Objective 7:** Define a plan on how the H2020 IoT-01-2016 LSPs and the CSA on H2020 IoT-02-2016 can use and apply the AIOTI WG03 recommendations (ongoing)
- **Objective 8:** Identify possible sustainable strategies for effective industry-wide deployment of the IoT standards (started).



AIOTI WG03 engagement model



- WGs support to AIOTI in:
- Digital Single Market
 - Digitising European Industry
 - EC's H2020 Large Scale Pilots

IoT SDOs and Alliances Landscape (Technology and Marketing Dimensions)



Source: AIOTI WG3 (IoT Standardisation) – Release 2.7

IoT SDOs and Alliances Landscape (Vertical and Horizontal Domains)

Home/Building

Manufacturing/
Industry Automation

Vehicular/
Transportation

Healthcare

Energy

Cities

Wearables

Farming/
Agrifood

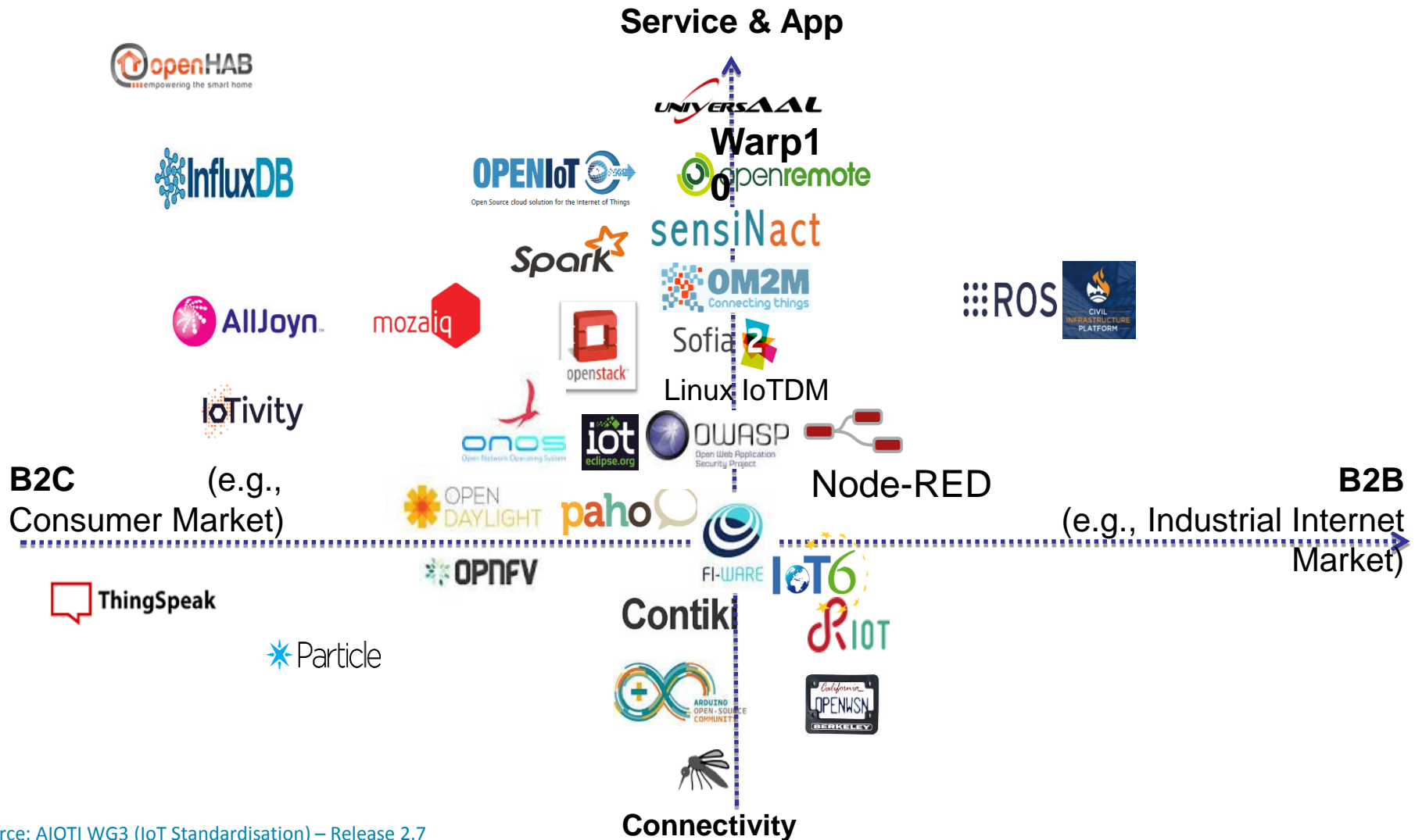
Source: AIOTI WG3 (IoT Standardisation) – Release 2.7

Horizontal/Telecommunication



AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

IoT Open Source Initiatives Landscape (Technology and Marketing Dimensions)



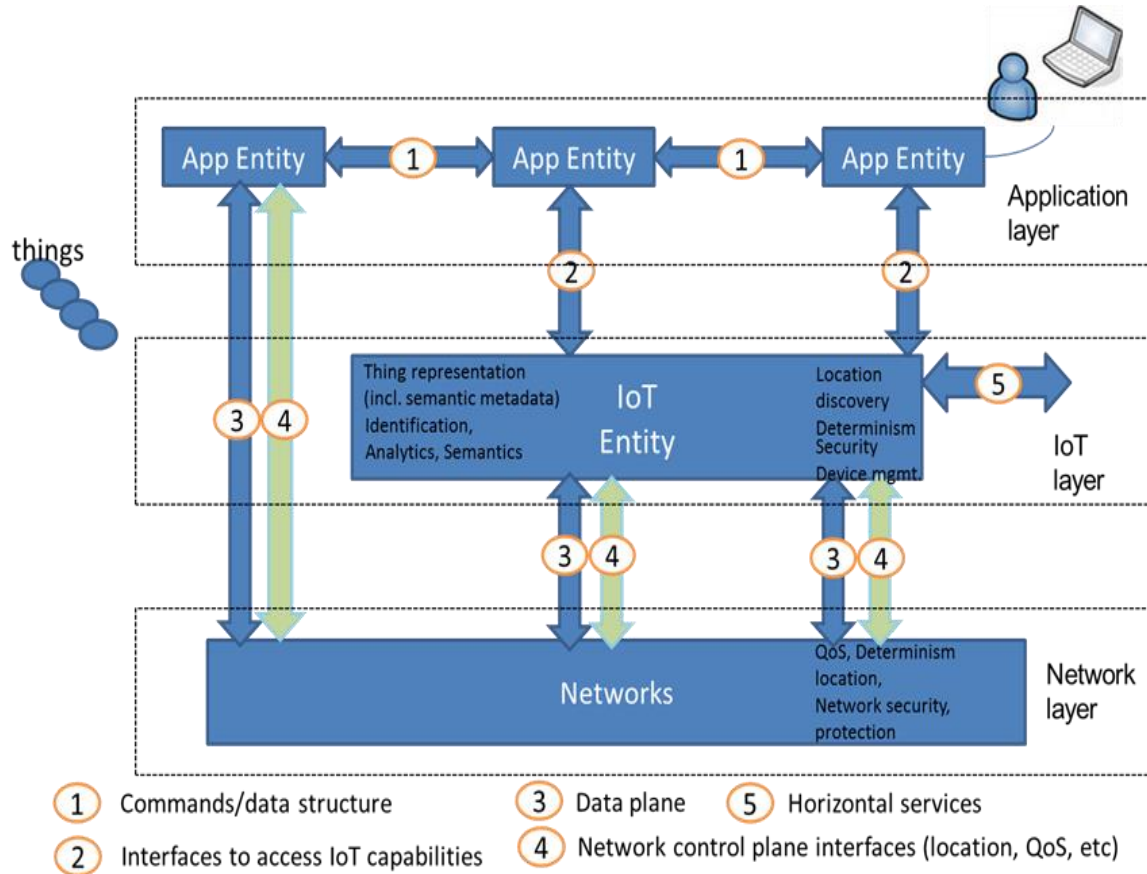
Source: AIOTI WG3 (IoT Standardisation) – Release 2.7



AIOTI

ALLIANCE FOR INTERNET OF THINGS INNOVATION

WG 03 High Level Architecture (HLA)



« HLA is open » - Topics for HLA v3

- ❖ HLA relationship to big data frameworks
- ❖ Mapping to other IoT architectures (e.g. RAMI 4.0, see next)
- ❖ Impact of virtualization (established contact with ETSI NFV vice chair, Marie-Paule Odini, HPE)
- ❖ Improve link to semantic interop (recommendations from joint AIOTI, IEEE, W3C and oneM2M white paper:
 - ❖ Feedback from LSPs
 - ❖ Use 42010 as a set of guidelines to address the work
 - ❖ STF505 gaps analysis
 - ❖ Collaboration with IIC and related testbeds, input from Agriculture Electronic Foundation, etc.
- ❖ IoT Identifiers (needs, requirements, landscape & gaps as a separate document)



WG 03 Semantic Interoperability

Recent achievements ->

- Collaboration with IEEE, oneM2M, W3C resulted in the publication of a [Joint Whitepaper](#)
- Supports WG3 objective of engagement with SDOs, Alliances, etc. and provides a platform for future cooperation
- Joint White Paper defines shared vision and challenges

Next steps ->

- Establish working relationship with LSPs to explore their respective needs for semantic interoperability
- Evaluate needs against shared vision and landscape (technologies, standards)
- Formulate recommendations as input to HLA
- Engage with SDOs, Alliances to align recommendations in a broader context



WG3 Privacy in IoT

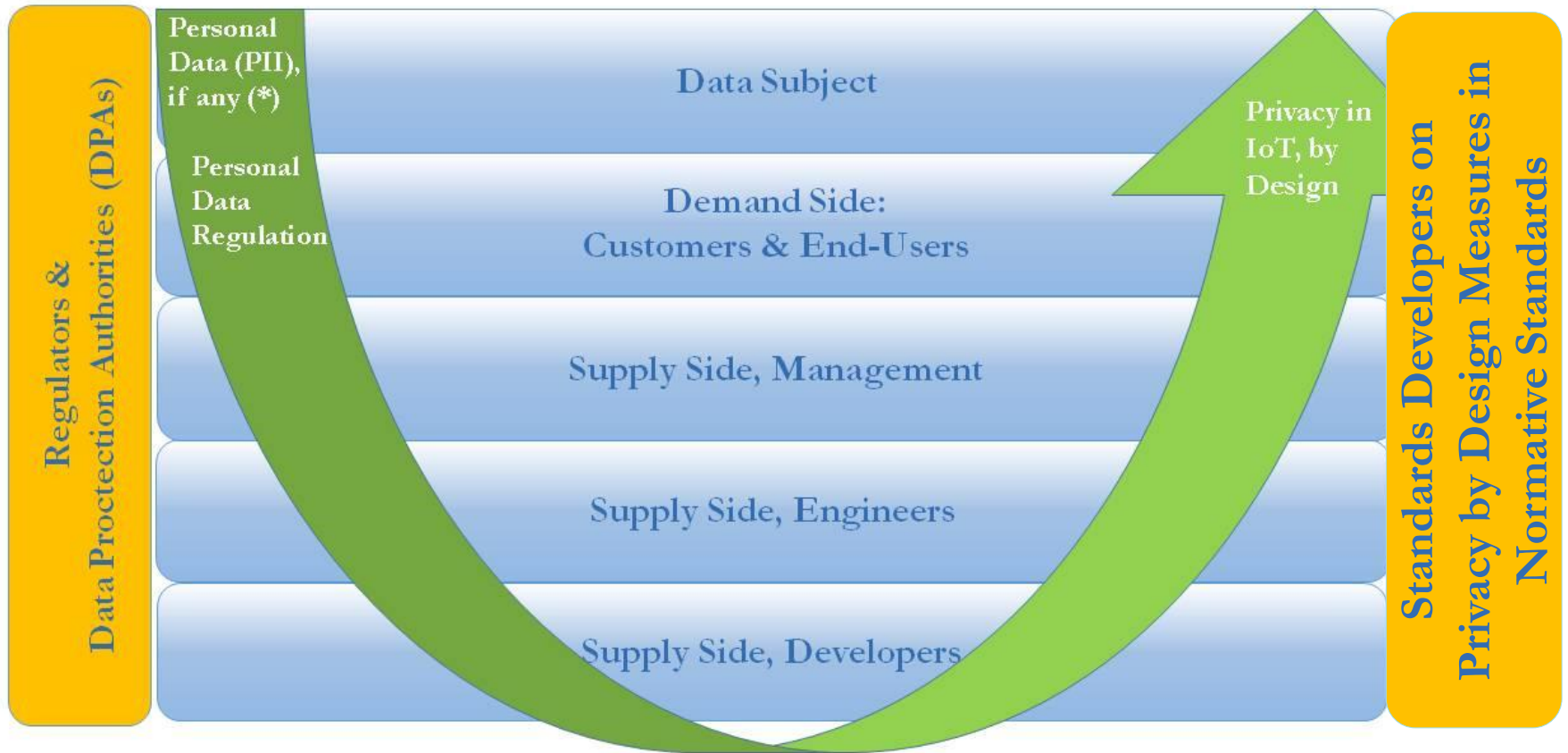
- ❖ Providing recommendations regarding personal data processing, management & protection to the various categories of stakeholders in an IoT undertaking:
 - **Demand side stakeholders:**
 - a set of guidelines for the demand side stakeholders who need to ensure that personal data protection concerns are taken into account in the supply chain and use of IoT
 - **Supply side stakeholders:**
 - set of guidelines for the managers who will integrate the practice of privacy-by-design in their organisations
 - technical set of guidelines for the engineers who will build the system so that the deployed system (**device (IC/FW/IFs/SW), communication, application, cloud and related processes**) can comply with privacy regulations
 - guidance for standards developers in provision of privacy by design measures in normative standards



WG3 Privacy in IoT

Privacy High Level Ecosystem in IoT

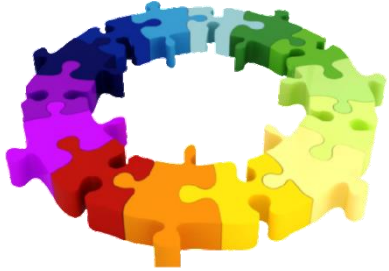
Main Categories of Stakeholders in Privacy in IoT



WG3 Security in IoT

- ❖ Within the AIOTI WG03 spirit and framework, **providing overview and recommendations regarding cyber-physical security and cybersecurity** (hereinafter collectively: ‘Security’) to the various categories of stakeholders in the various IoT ecosystems, in an IoT segmented/layered approach, **both from the demand side, supply side and authorities perspective**, including without limitation LSP stakeholders:
 - **Collecting & Structuring Security Repository** of **applicable regulations, standards, technical and organisational guidelines**, principles, frameworks, schemes, references and other best practices on Security, risks, impact, related classifications and measurement
 - **Landscaping** of Security Repository set above:
 - ❖ **Identifying & structuring Security classification categories** (such as devices, ecosystems, data, vulnerabilities, threats, risk and impact), and Classification per Category
 - ❖ **Identifying & Structuring Security needs and related requirements**
 - **Mapping, Identifying Gaps, Divergences & Commons Concerns** of the Security Landscapes
 - **Drafting & Disseminating IoT Security Framework, Recommendations & Guidelines:**
 - ❖ **to address Security concerns in IoT architectures and ecosystems**, including all layers in the applicable IoT verticals and horizontals are taken into account **design and engineering principles**, co-development, integration, testing, exploitation, deployment, use, monitoring security patching and end-of-life management of such IoT ecosystems
 - ❖ **to facilitate the practice of Security-by-design and compliance**
 - ❖ **to guide standards developers in provision of Security measures in normative standards**





AIOTI

ALLIANCE FOR INTERNET OF THINGS INNOVATION

Thank you!

www.aioti.org

#AIOTI



AIOTI

ALLIANCE FOR INTERNET OF THINGS INNOVATION