Project Acronym:	**VICINITY**
Project Full Title:	**Open virtual neighbourhood network to connect intelligent buildings and smart objects**
Grant Agreement:	**688467**
Project Duration:	**48 months (01/01/2016 - 31/12/2019)**

Deliverable D2.1

Analysis of Standardisation Context and Recommendations for Standards Involvement

Work Package:	**WP2 – Standardization analysis and VICINITY platform conformity**
Task(s):	**T2.1 – Analysis of IoT platforms, infrastructures, ontologies and Standards**
Lead Beneficiary:	**CAL**
Due Date:	**30 September 2016 (M9)**
Submission Date:	**30 September 2016 (M9)**
Deliverable Status:	**Submission to the EC**
Deliverable Type:	**R**
Dissemination Level:	**PU**
File Name:	**VICINITY_D2.1_Standardisation.pdf**

European Commission | Horizon 2020
European Union funding
for Research & Innovation

This project has received funding from the European Union's Horizon 2020 Research and innovation programme under Grant Agreement n°688467

VICINITY Consortium

No	Beneficiary		Country
1.	TU Kaiserslautern (Coordinator)	UNIKL	Germany
2.	ATOS SPAIN SA	ATOS	Spain
3.	Centre for Research and Technology Hellas	CERTH	Greece
4.	Aalborg University	AAU	Denmark
5.	GORENJE GOSPODINJSKI APARATI D.D.	GRN	Slovenia
6.	Hellenic Telecommunications Organization S.A.	OTE	Greece
7.	bAvenir s.r.o.	BVR	Slovakia
8.	Climate Associates Ltd	CAL	United Kingdom
9.	InterSoft A.S.	IS	Slovakia
10.	Universidad Politécnica de Madrid	UPM	Spain
11.	Gnomon Informatics S.A.	GNOMON	Greece
12.	Tiny Mesh AS	TINYM	Norway
13.	HAFENSTROM AS	ITS	Norway
14.	Enercoutim – Associação Empresarial de Energia Solar de Alcoutim	ENERC	Portugal
15.	Municipality of Pylaia-Hortiatis	MPH	Greece

Disclaimer
This document reflects only the author's views and the European Union is not liable for any use that may be made of the information contained therein.

Authors List

Leading Author (Editor)			
Surname	**First Name**	**Beneficiary**	**Contact email**
Dickerson	Keith	CAL	keith.dickerson@mac.com

Co-authors (in alphabetic order)				
No	**Surname**	**First Name**	**Beneficiary**	**Contact email**
1.	Heinz	Christopher	UNIKL	heinz@cs.uni-kl.de
2.	García -Castro	Raúl	UPM	rgarcia@fi.upm.es
3.	Sveen	Flemming	HITS	flsveen@online.no
4.	Tryferidis	Athanasios	CERTH	thanasic@iti.gr
5.	Hovstø	Asbjørn	HITS	hovsto@online.no
6.	Kostelnik	Peter	IS	peter.kostelnik@intersoft.sk
7.	Paralič	Marek	IS	marek.paralic@intersoft.sk
8.	Oliveira	Joao	ENERCOUTIM	j.oliveira@enercoutim.eu

Reviewers List

List of Reviewers (in alphabetic order)				
No	**Surname**	**First Name**	**Beneficiary**	**Contact email**
1.	Rico	Juan	ATOS	juan.rico@atos.net
2.	Nilsen	Rolv Moll	TINYM	rmn@tiny-mesh.com
3.	Vinkovic	Saso	GRN	saso.vinkovic@gorenje.com

Revision Control

Version	Date	Status	Modifications made by
0.1	30 March 2016 (M3)	Initial Draft	Keith Dickerson (CAL)
0.2	18 June 2016	First Draft formatted with contributions received	Keith Dickerson (CAL)
0.3	16 September 2016	Deliverable version for final review by partners	Keith Dickerson (CAL)
0.4	21 September 2016	Final improvements	Keith Dickerson (CAL)
0.5	25 September 2016	Deliverable version uploaded for Quality Check	Keith Dickerson (CAL)
0.6	29 September 2016	Outcome of Quality Check	Keith Dickerson (CAL)
0.6	30 September 2016	Final Draft reviewed	Christoph Grimm (UNIKL)
1.0	30 September 2016	Submission to the EC	Christoph Grimm (UNIKL)

Table of Contents

List of Tables

List of Figures

List of Definitions & Abbreviations

Abbreviation	Definition
AI	Artificial Intelligence
AIOTI	Alliance for Internet of Things Innovation
ANEC	European Association for the Co-ordination of Consumer Representation in Standardisation
ARIB	Association of Radio Industries and Businesses (Japan)
ATIS	Alliance for Telecommunications Industry Solutions
AWS	Amazon Web Services
bSDD	buildingSMART Data Dictionary
BSI	British Standards Institute
CCSA	China Communications Standards Association
CECED	European Committee of Domestic Equipment Manufacturers
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CIM	Common Information Model
CoAP	(IETF) Constrained Application Protocol
CoRE	(IETF) Constrained RESTful Environments WG
DICOM	Digital Imaging and Communications in Medicine
DSM	Demand Side Management
EC	European Commission
ECOS	European Environmental Citizens Organisation for Standardisation
ESO	European Standards Organisation
ETSI	European Telecommunications Standards Institute
EU	European Union
EV	Electric Vehicle
FG	Focus Group
GTM	GoToMeeting
HBES	Home and Building Electronic Systems
HL7	Health Level 7 International
HTTP	Hypertext Transport Protocol
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers Standards Association

IETF	Internet Engineering Task Force
IG	Interest Group
IHE	Integrating the Healthcare Enterprise
IoT	Internet of Things
ISO	International Organization for Standardization
ITS	Intelligent Transport Systems
ITU	International Telecommunications Union
LBD	Linked Building Data
M2M	Machine-to-Machine
MAS	(oneM2M) Management Abstraction and Semantics
MQTT	Message Queuing Telemetry Transport
NSO	National Standards Organisation
nZEB	Nearly Zero Energy Building
OASIS	Advancing open standards for the information society
OGC	Open Geospatial Consortium
OIC	Open Interconnect Consortium
OPC	Open Platform Communications (formally known as Object Linking and Embedding for Process Control)
OWL	W3C Web Ontology Language
PAS	Publicly Available Specification
PET	Privacy Enhancing Technology
RAML	RESTful API Modeling Language
RDF	(W3C) Resource Description Framework
REST	Representational State Transfer
RESTful	A service based on REST
SAB	(VICINITY) Stakeholder Advisory Board
SAREF	Smart Appliances REFerence ontology
SAWSDL	Semantic Annotations for WSDL and XML Schema
SDO	Standards Developing Organisation
SDW	(W3C) Spatial Data on the Web
SenML	Sensor Markup Language
SensorML	Sensor Model Language
SEP	Smart Energy Profile
SG20	ITU-T Study Group on IoT and its applications including smart cities and communities

SNRA	Sensor Network Reference Architecture
SoC	System on a Chip
SSCC-CG	CEN/CLC/ETSI Smart & Sustainable Cities & Communities Coordination Group
SSN	(W3C) Semantic Sensor Network
SUMO	(IEEE) Suggested Upper Merged Ontology
TIA	Telecommunications Industry Association
TNO	Netherlands Organisation for applied scientific research
TS	Technical Specification
TSDSI	Telecommunications Standards Development Society, India
TTA	Telecommunications Technology Association (Korea)
TTC	Telecommunication Technology Committee (Japan)
TTP	Trusted Third Party
UML	Unified Modelling Language
URI	Uniform Resource Identifier
USEF	Universal Smart Energy Framework
W3C	World Wide Web Consortium
WG	Working Group
WoT	Web of Things
WSML	Web Service Modelling Language
WSMO	Web Service Modelling Ontology
XDR	(IETF) External Data Representation
XML	eXtended Markup Language
ZCL	ZigBee Cluster Library

Executive Summary

This document is a deliverable of the VICINITY project [1], funded by the European Commission (EC) Directorate-General for Research and Innovation (DG RTD), under the ICT-30 IoT action [2] of its Horizon 2020 Research and Innovation Programme (H2020).

Section 2 examines the architecture of the VICINITY project and the options for hardware, software and middleware that could be implemented. This information is then used to identify the standards requirements of VICINITY in Section 3 including the requirements of the hardware and software platforms, the VICINITY architecture and the 3 pilots that are being set up to test the interoperability of VICINITY gateways and devices reported in Section 4.

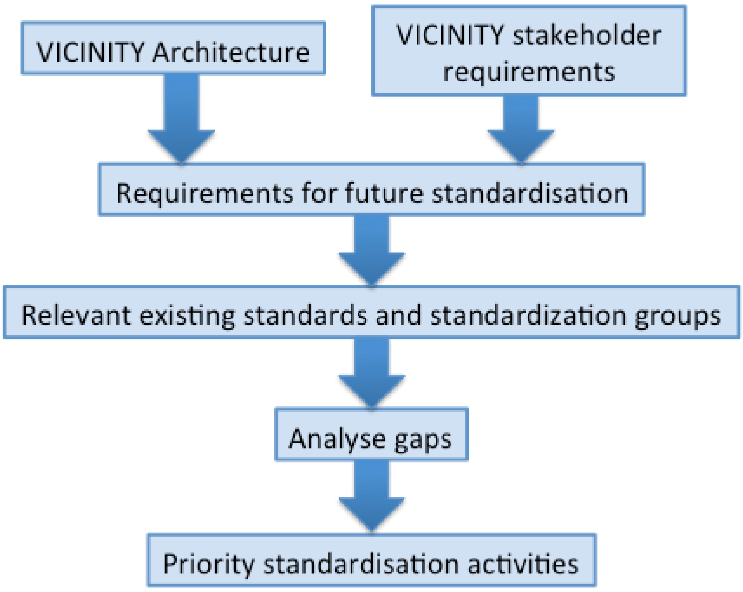
Section 5 identifies the standards bodies that are relevant to the VICINITY project at all levels. These include bodies developing formal standards at European level, such as CEN, CENELEC and ETSI, and at International level such as ISO, IEC and ITU. However, equally important to VICINITY are fora and consortia with worldwide membership, such as OIC and W3C, and also industry associations such as the European Committee of Domestic Equipment Manufacturers (CECED). The bodies that VICINITY partners currently participate in are also identified.

Section 6 provides recommendations on the standards bodies, fora and consortia that VICINITY partners should participate in and the objectives that they will follow to meet the specified requirements. A major focus will be on the standardisation of ontologies that are being defined in bodies such as oneM2M, ETSI SmartM2M and W3C. Specific requirements of the pilots will be met in bodies such as the Continua Health Alliance and ISO/IEC JTC1. Other bodies will be monitored for developments relevant to VICINITY.

1 Introduction

The establishment of a common IoT ecosystem will be a major contribution to the EU Connected Digital Single Market [3].

The process shown in Figure 1 was used to identify the standards that are important to VICINITY and the priority areas for participation in relevant standardization bodies. It identifies current standards development that is most relevant to VICINITY (and most likely to be able to use VICINITY input effectively). Recommendations are then made on which standards working groups (WGs) that VICINITY partners should contribute to so that these meet VICINITY requirements. VICINITY will also support proposals for new standards that could help develop the market for VICINITY services.


VICINITY Architecture

VICINITY stakeholder requirements

Requirements for future standardisation

Relevant existing standards and standardization groups

Analyse gaps

Priority standardisation activities

Figure 1: Process to identify VICINITY standards involvement

However, the temptation to create new standards where gaps are identified must be resisted unless absolutely necessary for the reasons highlighted in Figure 2. The aim should always be to re-use existing standards wherever possible and to propose extensions or modifications to these if they can't be used as they are. The creation of completely new standards would consume a large amount of project resources and should not be undertaken lightly. In particular, the creation of a new standards development group would use a significant proportion of VICINITY resources that are assigned to standards development and may be counter-productive anyway for the reasons given in Figure 2. Therefore, creation of a new standards group should only be done as a last resort and in conjunction with other H2020 IoT-EPI projects if VICINITY objectives can not be met in any other way.

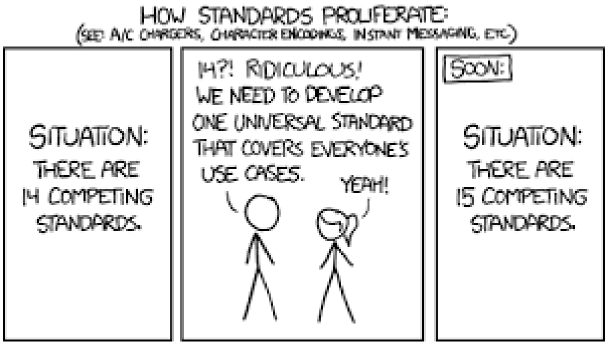

HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

Figure 2: Why standards proliferate.

Standards groups, fora and consortia relevant to IoT and VICINITY are identified in Section 5. The project does not have the resources to participate in all of these, and so we must identify the groups where VICINITY can add most value in order to meet project objectives.

2 VICINITY Architecture & Hardware/Software Platforms

This section examines the architecture of the VICINITY project and the options for hardware software and middleware that could be implemented. This information is then used to identify standards requirements in Sections 3. The requirements of the pilots are identified in Section 4 and the Standards bodies that are working in relevant areas are examined in Section 5.

A simplified VICINITY architecture is shown in Figure 3.

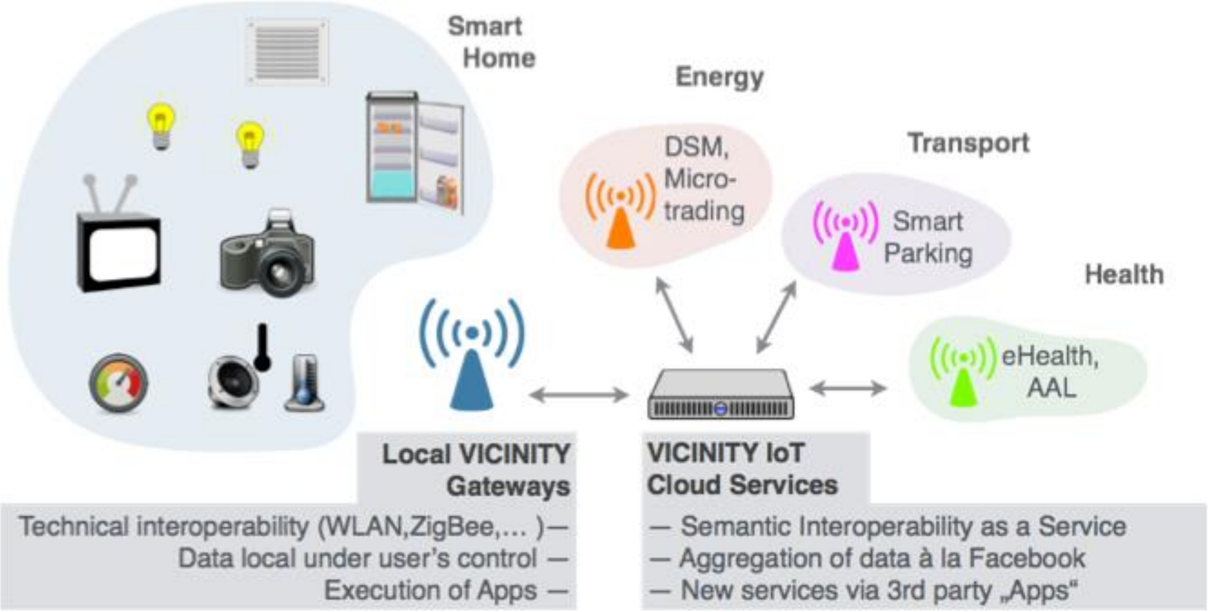

Smart Home
Energy
DSM, Micro-trading
Transport
Smart Parking
Health
eHealth, AAL
Local VICINITY Gateways
VICINITY IoT Cloud Services
Technical interoperability (WLAN,ZigBee,…)—
Data local under user's control —
Execution of Apps —
— Semantic Interoperability as a Service
— Aggregation of data à la Facebook
— New services via 3rd party „Apps"

Figure 3: VICINITY User Platform

2.1 Survey of IoT Hardware/Software Platforms

Nowadays the electronics market offers all kinds of hardware devices, starting from simple microcontroller boards and ending with complex hardware development kits. They mainly follow the requirements of low power and small size. To a good extent these requirements are fulfilled by communication technologies and standards such as radio-frequency identification (RFID), quick response (QR) codes, Bluetooth low energy (BLE) technology, WiFi direct, IEEE 802.11ah (HaLow), etc. Moreover, the relatively young market of home automation electronics offers new technologies like Z-Wave, ZigBee or HomePlug, which pursue the same challenges.

As a result, the world of embedded devices is full of different kinds of smart devices, which use vast amounts of all possible communication protocols and standards and their modifications. Their integration in terms of IoT is supposed to be performed by IoT gateways.

The main objective of IoT gateways is to connect heterogeneous devices with each other and with the Internet. These devices might all use different wired and wireless communication protocols and for various reasons (usually energy saving) do not have appropriate network interfaces (Ethernet, WiFi).

For use as an IoT gateway a universal device is needed that is fast, reliable, with a huge amount of interfaces (or easy extendable), energy-saving and cheap. On top of this hardware, a software framework/platform is required in order to enable autonomic networking, security/privacy features and manageability.

Thus, the functionality that an IoT gateway should provide, includes:

- Device discovery
- Identification-based connectivity
- Interoperability
- Plug-and-Play
- Security and privacy
- Manageability
- Location-based capabilities

Support for semantic interoperability is limited and specific to standards (e.g. ZigBee Profiles).

Chapter 3 gives an overview of standards that enable interoperability at a higher, semantic layer.

2.1.1 Comparison of available Hardware Platforms

To match the requirements for an IoT Hardware Platform, the following candidates have been considered:

- **Banana Pro**: An open-source single-board computer, developed by LeMaker (China) and released in October 2014. It is based on AllWinner A20 System on a Chip (SoC), has 1GB of DDR3 memory and can run a large number of different operating systems: Lubuntu, Android, Debian, Bananian, Berryboot, OpenSuse, Scratch, Fedora, Gentoo, Open MediaVault, OpenWRT and BSD [4]. As long as Banana Pro is actually the advanced version of Banana PI, a lot of software originally developed for Banana PI could be also used with Banana Pro.
- **Cubieboard 3 (Cubietruck)**: An open-source single-board computer released in October 2013 by CubieTeam (China). Like Banana Pro, it also uses AllWinner A20 SoC, but models with 1GB or 2GB of DDR3 memory also exist. Cubietruck can run the following operating systems: Android, Cubieez, Lubuntu and Fedora [5].
- **Raspberry PI 3 Model B**: Nowadays the most famous single-board computer, developed in the UK by the Raspberry PI Foundation. It has 1GB of DDR2 memory, and in comparison with Banana Pro and Cubieboard 3, it uses 64-bit Broadcom SoC of the next generation. Raspberry PI is designed to run the Raspbian operating system, but there Ubuntu, Pidora, OpenELEC, RISC OS and Windows 10 are also possible OS. The Raspberry PI Series in general has a very large and active open source community. Most Applications and extension hardware developed for any of the previous Raspberry Pi Boards is also compatible with the Raspberry Pi 3. This compatibility is one major aspect that makes the Raspberry Pi successful. It is most likely to continue with potential future Revisions of this series, making it ideal, when it comes to upgrades, also when used as an VICINITY gateway.
- **Pine A64**: the young project of a single-board computer, developed by a team of designers, engineers, and entrepreneurs from the USA. It was released in February 2016, and it uses AllWinner A64 System on a Chip, which has the same CPU architecture as the Broadcom SoC in Raspberry PI. There exist models with 1GB or 2GB of DDR3 memory. It can run Android, Remix OS, Ubuntu, Arch Linux and Windows 10. Pine A64 has two very important advantages: from all considered boards, this is the cheapest one, and it is fully compatible with Raspberry PI 2 extension boards [6]. The PINE A64 is a very young project, with a community yet relatively small, but likely to

grow in the near future. Its major advantage is the capability to not only run Linux, but also Android as an Operating System, which is supported and actively maintained by its community.

- **Intel Edison**: This is the response of Intel to the IoT ecosystem of different like-mini-pc options in the market. It is a good alternative to Raspberries with the advantage of using an x86 chipsets which facilitate developments and deployment of software. It is covered with a wide community of support and developers. At the same time provides an interface to integrate an Arduino board, a great option to prepare faster prototypes. 40 GPIO interfaces that allows to prototype IoT devices and gateways.

More detailed specifications of the considered hardware platforms are shown in Table 1.

In summary all of the presented hardware platforms are suitable choices as an IoT gateway, when it comes to performance and extendability. The Raspberry Pi 3 has most likely the largest support in open-source community and might hence be the favourable choice to attract the most stakeholders to join the VICINITY. Still the other presented solutions have their advantages as well and a final decision has to made according to the Requirements of the VICINITY Pilot sites as further discussed in Deliverable D1.3. [7][8]

	Banana Pro	Cubieboard (Cubietruck)	Raspberry Pi 3 Model B	PINE64+ 2GB	Intel Edison (EDI2ARDUIN.AL.K)
SoC	Allwinner A20	Allwinner A20	Broadcom	Allwinner A64	Intel® Atom™ processor
CPU	1 GHz ARM Cortex-A7 Dual-Core	1 GHz ARM Cortex-A7 Dual-Core	1.2 GHz ARM Cortex-A53 Quad Core	64bit Quad Core ARM A53 1.2GHz CPU	dual-core processor at 500 MHz
Memory	1GB DDR3@432 MHz	2 GB DDR3@480 MHz	1GB DDR2@450 MHz	2 GB DDR3	1 GB DDR3 RAM, 4 GB eMMC Flash
Graphic engine	Mali400MP2, compatible with OpenGL ES 2.0/1.1 (hardware acceleration support)	Mali400MP2	Broadcom VideoCore IV	Mali400MP2	-
Audio output	Yes	Yes	Yes	Yes	No
Audio input	Yes	Yes	No	Yes	No
HDMI	Yes	Yes	No	Yes	No
Camera Interface	Yes, 1 x Parallel 8-bit camera interface	No, USB-camera is possible	Yes	Yes	GPIO Interface
Micro-SD slot	Yes	Yes	Yes	Yes	Yes
Expansion header	40-pin header, 28xGPIO, can be used for UART, I2C, SPI, PWM, CAN, I2S, SPDIF	54 pins including I2S, I2C, SPI, CVBS, LRADC x2,UART, PS2, PWM x2, TS/CSI, IRDA, LINEIN&FMIN&MICIN, TVIN x4 with 2.0 pitch connectors	40-pin GPIO	Euler "e" bus, Raspberry Pi 2 Bus	40 GPIO interface
External interface	2 x USB Host 1 x USB OTG	2 x USB Host 1 x OTG	4 (from 5-port USB-hub)	2 x USB 2.0 host port	2x USB 2.0
SATA	2.0	2.0	No	No	No
Ethernet	10/100/1000Mbps	10M/100M/1000Mbps	100 Mbps	1 Gbps	No
WiFi	Yes	Yes	Yes	Yes	Yes
Bluetooth	No	Yes	Bluetooth 4.1 BLE	Yes	Bluetooth 4.0
ZigBee	No	No	No	No	No
Other	IR receiver	IR receiver, 8 GB NAND-Flash		3-pin connector for lithium battery, 2-pin connector for RTC clock, Touch panel connector, Display DSI connector, optionally Z-Wave	UART, I2C, I2S, GPIO Additional 12 (with 4 capable of PWM)
Price	43 - 46 €	93 - 104 €	37.50 €	25 €	100€

Table 1: Comparison of available Hardware platforms.

2.1.2 Comparison of available Software Frameworks

Selection of a hardware platform alone does not solve the requirements for an IoT Gateway. One of the following IoT Software Frameworks is also needed on top of the specified hardware:

- **OpenHAB SmartHome Framework**: This open source project is one of the most widely known solutions for IoT gateways. It was developed to simplify home automation, but because of its modular OSGi architecture and the variety of supported protocols [9] it can be also used as an IoT gateway.

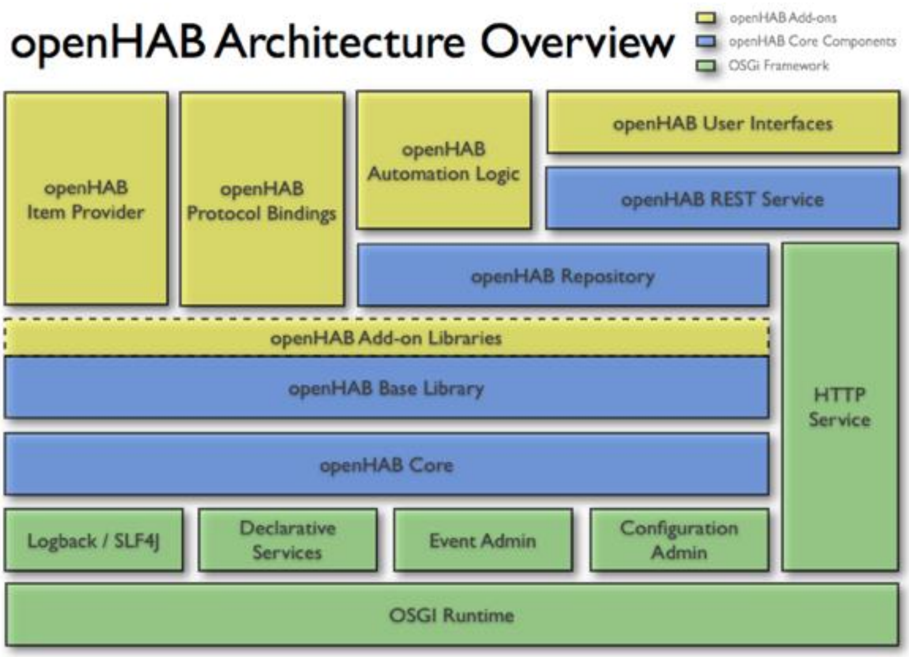


Figure 4: openHAB Architecture Overview

The openHAB runtime is a set of OSGi bundles deployed on the OSGi framework "Equinox". It is therefore a pure Java solution and needs only a JVM to run [10]. The architecture of OpenHAB is shown in Figure 4. This provides a lot of flexibility because of its modular structure and it is possible to add and remove functionality during runtime without the need to stop the service. Functionality includes keeping track of the status of items, communication between services, sending commands to items. Everything communicates through an openHAB Event Bus so the connection between openHAB instances is kept as low as possible.

OpenHAB is absolutely vendor-neutral and protocol agnostic and can be easily accessed with mobile phone or web application. With openHAB it is possible to build an intranet inside a home, and no data will leave it, because the user has total control over it.

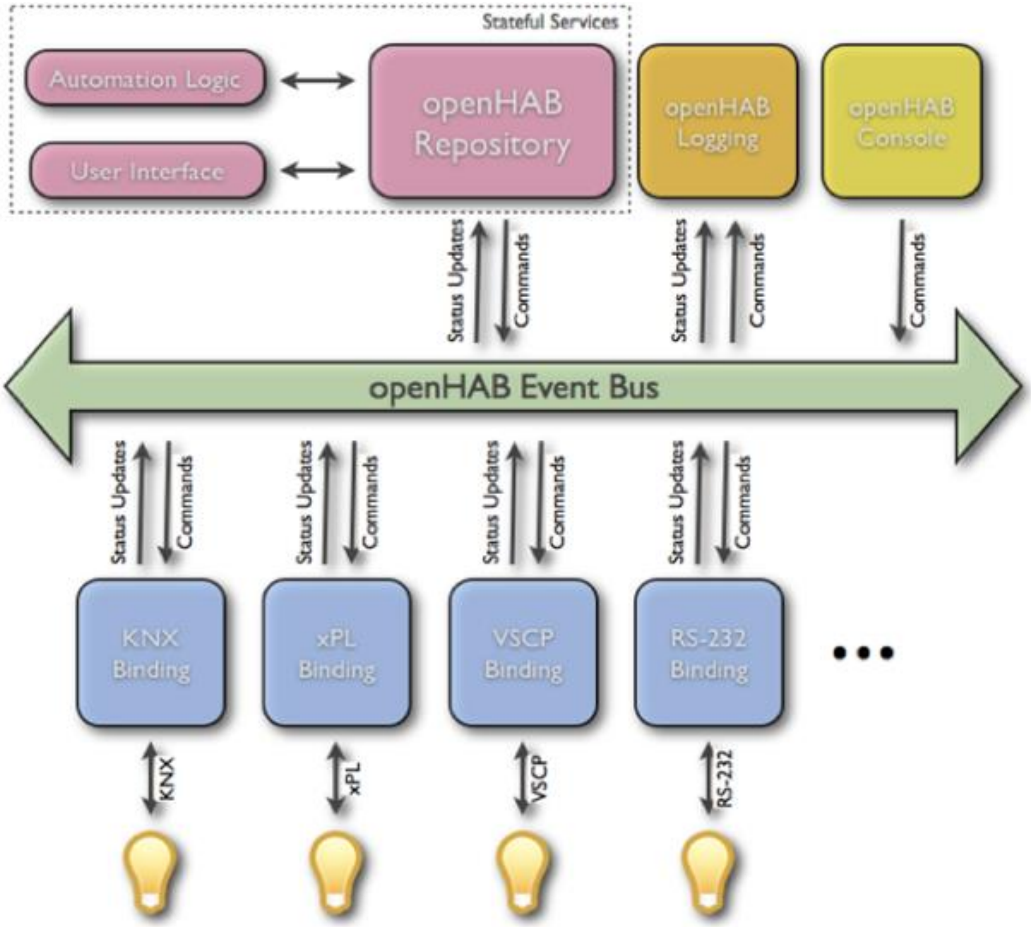


Figure 5: OpenHab as middleware

- **DeviceHive IoT Framework**: The cloud-based project DeviceHive does not use OSGi, nevertheless this framework for M2M communication provides all means for building Internet of Things. DeviceHive was mainly designed for enabling message exchange between smart devices and client applications. DeviceHive contains cloud services, open source server and client libraries, protocol adapters, examples, documentation, management system. The architecture of DeviceHive is based on D-BUS, so it can be used only on POSIX-compliant systems (see Figure 6).

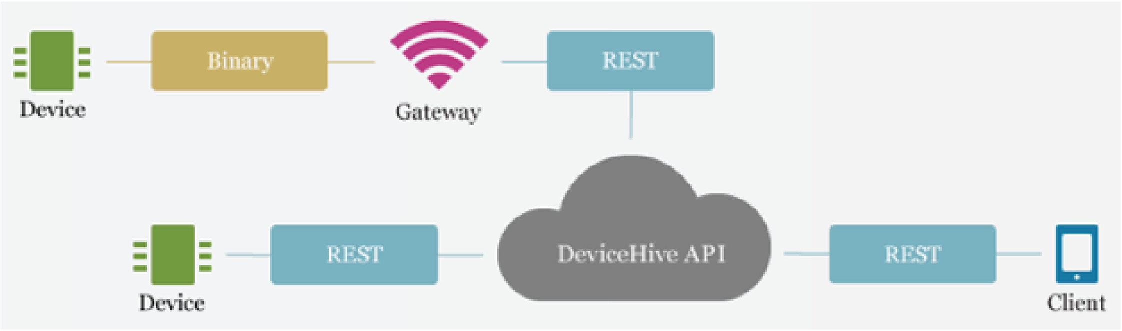


Figure 6: DeviceHive-based IoT system

DeviceHive is an AllSeen Alliance member, so it speaks AllJoyn providing cloud connectivity for AllJoyn devices and also bridges 3rd party protocols into AllJoyn expanding the ecosystem of supported devices. Thus, AllJoyn support comes out of the box and can be customized for various integration scenarios [11].

DeviceHive is well suited to usage in enterprise solutions and works in public and private clouds (OpenStack, Microsoft Azure, own datacenter, etc.). The most remarkable thing about DeviceHive is its lambda architecture, which implies enormous scalability.

- **OpenRemote**: Another one open source project, OpenRemote was started in 2009 with the goal of overcoming the problems caused by attempts at integration between different protocols and already existing M2M communication solutions. It consists of three parts: online designer, controller and panel or custom Android/iOS application (see Figure 7).

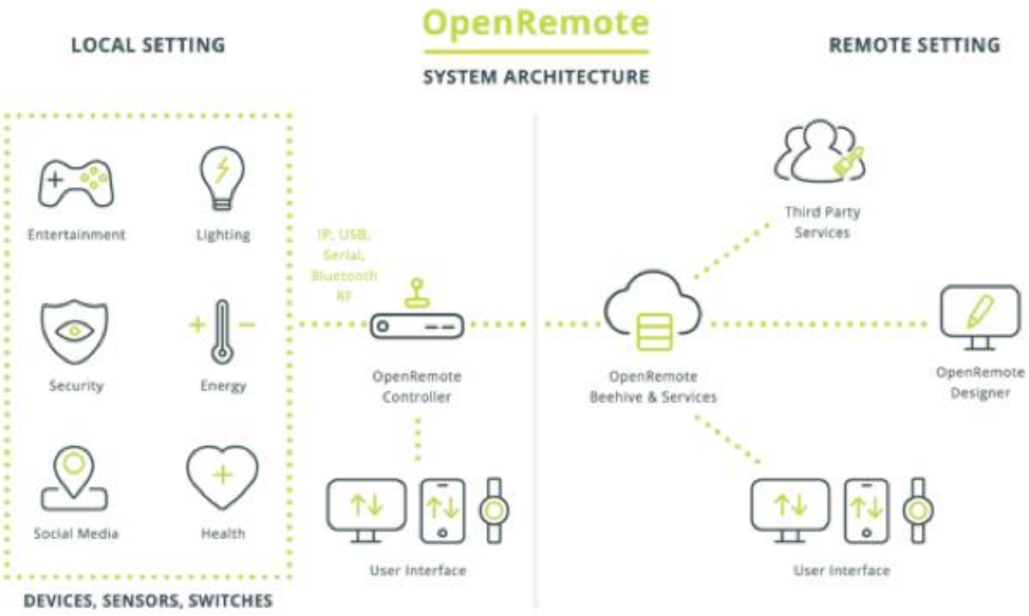


Figure 7: OpenRemote-based IoT system

Online Designer provides help to the Building Modeller to configure devices and internet services, define macros and write rules to automate the IoT system. Another part of online Designer, UI Designer, provides a way to design a user interface for a Web Browser, iOS or Android.

The OpenRemote Controller actually represents the gateway - it connects devices and services and runs the designed automation scripts. For controller purposes a variety of hardware can be used, for example, Raspberry Pi or BeagleBone.

The idea of the panel or Android/iOS custom application is to connect to the controller and display designed in online Designer interface. Users can see the status of connected devices or services via these Apps or a browser connection, and control the system using buttons, sliders, etc.

OpenRemote provides a centralized data and user account management, device configuration database and a variety of other management features. High scalability potential makes possible the usage in Industry, Health Care, Smart Cities [12]. As long as OpenRemote is fully written in Java, it has also very high portability and can be deployed on any Java 6 compatible platform.

- **AllJoyn**: Alljoin is a project supported by the AllSeen Alliance and has very high chance to become a worldwide standard. "AllJoyn is an open source software framework that makes it easy for devices and apps to discover and communicate with each other. Developers can write applications for interoperability regardless of transport layer, manufacturer, and without the need for Internet access" [13]. This framework can be used on all modern operating systems, since it offers an abstraction layer for Android, IOS, Linux and Windows. AllJoyn offers features such as easy discovery and group formation, the ability to share control among devices and applications and it is easy extendable to integrate with new protocols.

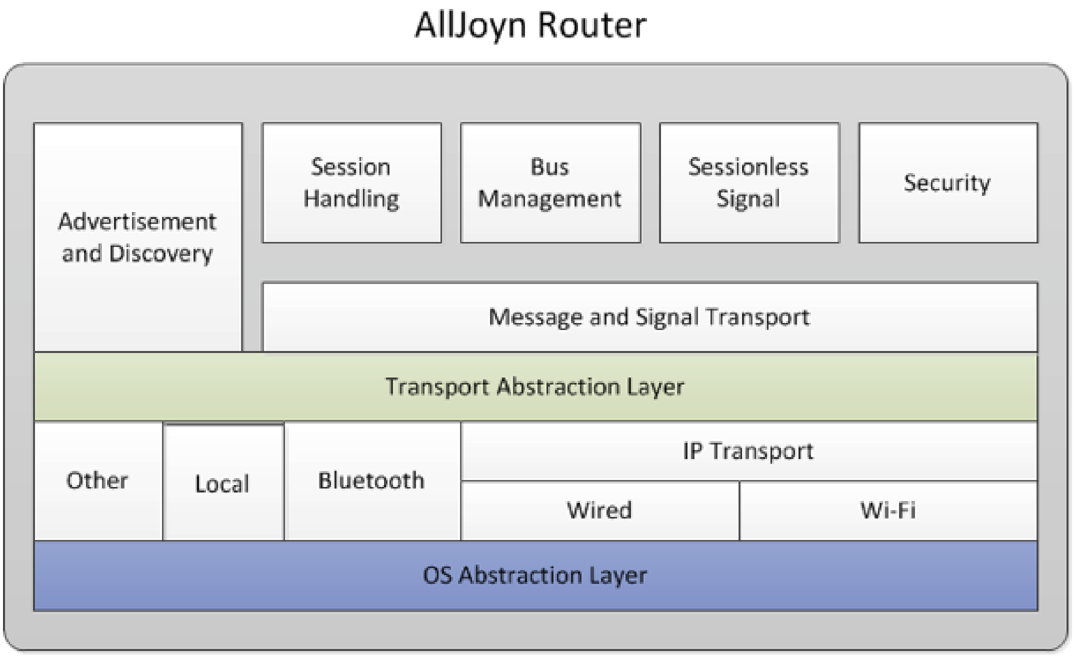


Figure 8: AllJoyn Router

- **Iotivity**: The Iotivity project was created in 2015 and so is younger than Alljoyn. However, it has the potential to become complementary to the Alljoyn framework:

  "The IoTivity project was created to bring together the open source community to accelerate the development of the framework and services required to connect these billions of devices. The IoTivity project is sponsored by the Open Connectivity Foundation (OCF), a group of industry leaders who will be developing a standard specification and certification program to address these challenges" [14].

  Iotivity has advanced discovery mechanisms and provides transparent data and device management possibilities. It can be installed on Android, Linux, IOS and Windows. Compared to Alljoyn, Iotivity offers a more simplified API to create Iotivity compliant Servers and Clients.

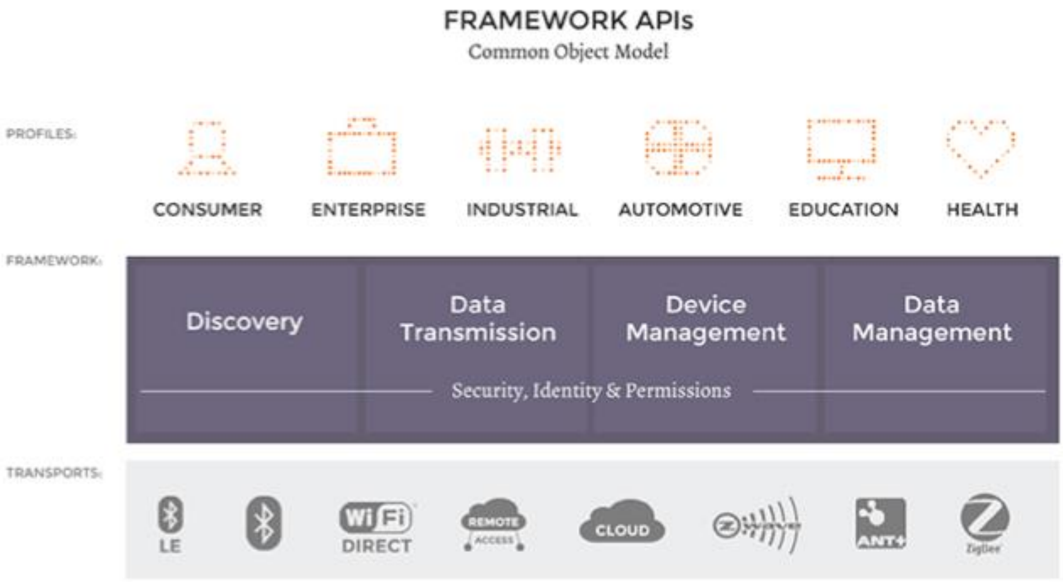


Figure 9: Iotivity Framework API

Finally, a direct comparison of the different software platforms mentioned above is shown in Table 2.

	OpenHAB	Device Hive	OpenRemote	AllJoyn	Iotivity
Platform	JVM	POSIX-compliant	JVM	Linux, Windows, Mac, Android	Linux, Android, IOS, Windows
Development language	Java	C/C++, Go, Java, Python, Bash	Java	C, C++, Java, objective-C	C/C++ Java (Android) JavaScript (in future)
Documentation clarity	4/5	4.5/5	5/5	4.5/5	5/5
Alliance members, partners, users	EnOcean Alliance, AllSeen Alliance, Eclipse Foundation	AllSeen Alliance	TU Eindhoven, NEEO, Philips, Trust, etc.	AllSeen Alliance	Open Internet Consortium
License	Eclipse Public License	MIT License	GNU AGPL	ISC License	Apache License 2.0

Table 2: Comparison of Software Frameworks.

2.2 Options for Middleware

In this section we will briefly characterise key features of selected IoT software platforms that represent potential platforms to be integrated via Vicinity approach. Before we start to analyse the features, let us rephrase the important features expected from an IoT Software Platform as they are listed in [15] and more detailed in [16]: device management, integration support, information security, protocols for data collection, types of analytics and support for visualizations.

IoT Platform should maintain a list of devices and key metadata information about them in order to offer data streams for IoT applications. As well it should be possible to configure these devices, change operational settings, upgrade their software remotely, querying the status and support reporting of any error conditions [16]. Key features of IoT platform (control & data access) should be made available to the outside world via APIs – nowadays it is common to use REST APIs. Protocols used by IoT Software Platforms could be distinguished according to [4] as application protocols (e.g. RTPS), payload container protocols (e.g. CoAP, SOAP), Messaging Protocols (e.g. AMQP, MQTT, XMPP, JMS) and Legacy Protocols (e.g. BACnet or UPnP). Type of data analytics used in IoT are real-time [17], batch on an accumulated set of data, predictive and interactive [18].

According to the Saverio Romeo, Principal Analyst at Beecham Research, there are more than 300 IoT platforms today [19]. It is beyond the scope of this deliverable to analyse all of these, even briefly. However, before selecting any of them, let us mention other current sources, where the IoT platforms are surveyed:

- 16 cloud-based IoT platforms are summarised in [20] (*Arrayent*, *Axeda*, *Bugswarm*, *Carriots*, *EvryThng*, *Exosite*, *GrooveStreams*, *IFTTT*, *Kaaproject*, *LinkSmart*, *Mbed*, *Nimbits*, *Particle.io*, *Autodesk SeeControl*, *SensorCloud*, *PTC ThingWorx*, *ThingSpeak*).
- Paper [15] analyses and identifies key features of 11 IoT Software Platforms (*2elemetry*, *Appcelerator*, *AWS IoT platform*, *Bosch IoT Suite*, *Ericsson Device Connection Platform*, Evrythng, *IBM IoT Foundation Device Cloud*, *ParStream*, *PLAT.ONE*, ThingWorx, *Xively*).
- [21] focuses on IoT software platforms that enable interoperability of different IoT solutions and compares 9 of these (*iCity*, *SmartSantander*, *OpenIoT*, *iCore*, *Spitfire*, *PLAY*, *StarCity*, *VITAL*, *CityPulse*).
- [22] evaluates 39 IoT middleware platforms focusing on usability (*AirVantage*, *Arkessa*, *ARM mbed*, Carriots, *DeviceCloud*, *EveryAware*, *Everyware*, EvryThng, *Exosite*, *Fosstrack*, *GroveStreams*, *H.A.T.*, *IoT-framework*, IFTTT, *Kahvihub*, LinkSmart, *MyRobots*, *Niagara*, *Nimbits*, *NinjaPlatform*, *Node-RED*, OpenIoT, *OpenMTC*, *OpenRemote*, *Open.Sen.se*, *realTime.io*, *SensorCloud*, *SkySpark*, *Swarm*, *TempoDB*, *TerraSwarm*, *The thing system*, *Thing Broker*, *ThingSpeak*, *ThingSquare*, ThingWorx, *WoTkit*, Xively)[1].

The following representative IoT platforms are described in more detail in the following sections:

- Amazon Web Services (AWS), an IoT platform that is often cited as the most popular industrial platform today,
- LinkSmart, a cloud-based IoT middleware that makes any device available as a service in an uniform way,

[1] Platforms already mentioned are written in roman

- OpenIot, an open source middleware platform enabling the semantic unification of IoT applications in the cloud.
- FIWARE, an enhanced OpenStack-based cloud environment plus a rich set of open standard APIs that make it easier to connect to the Internet of Things, process and analyse Big data and real-time media or incorporate advanced features for user interaction.

2.2.1 AWS IoT platform

The high-level functional, component and communication architectural views of an AWS IoT platform is shown in Figure 10 [23].

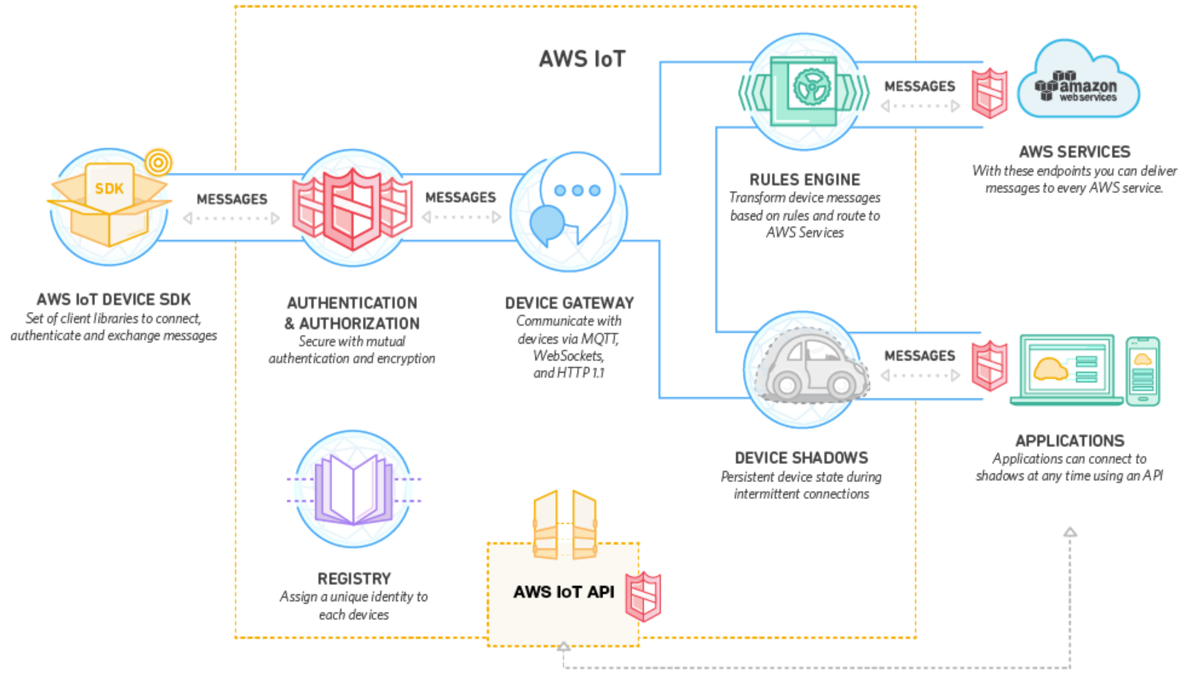

AWS IoT
SDK
AWS IoT DEVICE SDK
Set of client libraries to connect, authenticate and exchange messages
MESSAGES
AUTHENTICATION & AUTHORIZATION
Secure with mutual authentication and encryption
MESSAGES
DEVICE GATEWAY
Communicate with devices via MQTT, WebSockets, and HTTP 1.1
RULES ENGINE
Transform device messages based on rules and route to AWS Services
MESSAGES
amazon webservices
AWS SERVICES
With these endpoints you can deliver messages to every AWS service.
DEVICE SHADOWS
Persistent device state during intermittent connections
MESSAGES
APPLICATIONS
Applications can connect to shadows at any time using an API
REGISTRY
Assign a unique identity to each devices
AWS IoT API

Figure 10: High-level functional, component and communication architectural views of AWS IoT platform

For device management AWS IoT platform provides the registry service called Thing Registry that assigns unique identity to devices and resources associated with them. Besides unique identifier and authentication certificate, it enables to store up to three custom attributes associated with the resource (i.e. real device or virtual application).

The AWS IoT Device Gateway enables communication between devices and IoT services according to the publish/subscribe model – so not only one-to-one but also one-to-many communication. Currently it supports MQTT, WebSockets, and HTTP 1.1 protocols. Communication between devices and AWS IoT is always between parties with proven identity. MQTT uses certificate based authentication (X.509), and WebSockets connections can use SigV4. AWS IoT side use certificates generated either by the platform itself or any other preferred Certification Authority. All communication with AWS IoT message broker and shadow service is encrypted with TLS.

AWS IoT platform support real-time analytics by Rules Engine, Amazon Kinesis, AWS Lambda, where rules are analysed and actions are performed based on the MQTT topic stream. It is possible also to make predictions based on an Amazon ML model by sending the data from an MQTT message to Amazon Machine Learning.

AWS IoT offers possibility to create a virtual device (i.e. a shadow) that can hold and represent a persistent state of the device. In this way building of application is made easier by providing always available REST APIs, which are part of the AWS IoT Device SDK. SDK includes open source libraries, the developer guide with samples, and the porting guide. It enables to connect the devices with gateway and AWS services in secure way.

2.2.2 LinkSmart

The functional architecture of the LinkSmart platform is shown in Figure 11 [24].

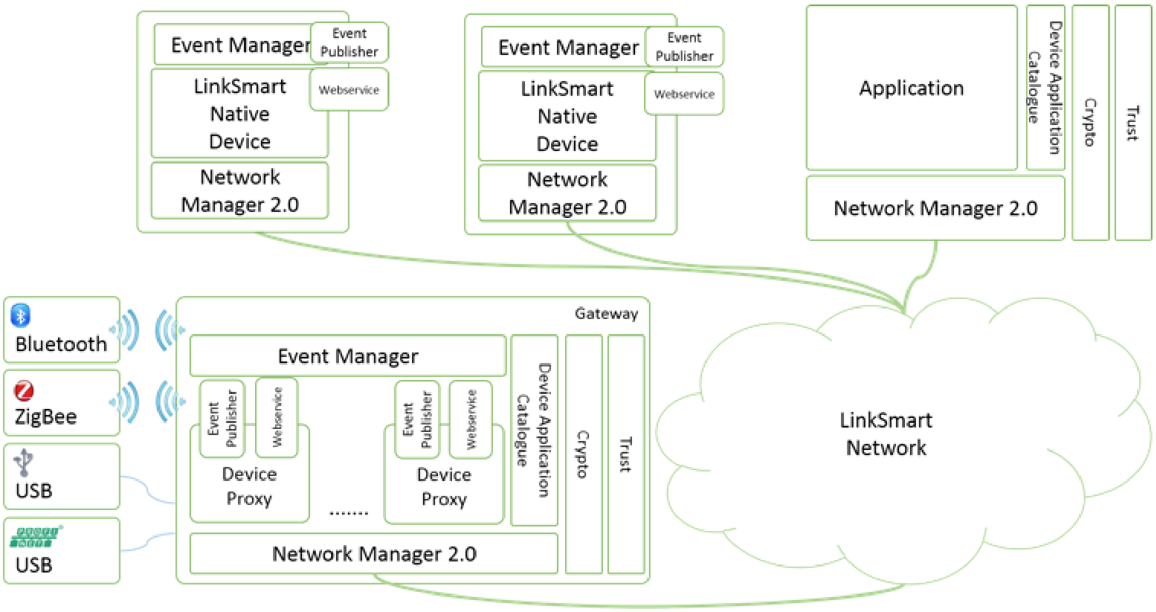


Figure 11: Functional architecture of the LinkSmart platform.

LinkSmart from the architectural point of view is middleware consisting of a set of loosely coupled managers supporting the following key features – networking, eventing, security, proxy discovery, proxy development and configuration. A device could be part of the LinkSmart network either as a native device or via proxy. Native device should be able to host the core managers for networking and eventing, as well as run web services to access this functionality. Constrained devices or closed platform/legacy devices could be part of the network via proxy running at a gateway (usually a PC with IP connectivity). The result is accessibility of every device as a web service.

Device management involves Network manager that implements Web Service over JXTA as the Peer-to-Peer model for device-to-device communication and Resource Catalogue. During the device registration process a 32-byte long virtual address (with format *contextID-3.contextID-2.contextID-1.serviceID*) of corresponding web service is created and stored together with description and a freely chosen set of attributes. Discovery process support not only virtual address based search, but also attribute based that utilises mapping of attributes to Bloom-filter. Resource Catalogue is responsible for discovering resources (i.e. devices, sensors, things) in local broadcast domain of the gateway, as well as for storing and maintaining information about them.

The Event Manager provides a topic-based publish-subscribe service in Linksmart. Which processes all non-functional properties-data for services/components, devices, and network.

The Crypto and Trust functions carry out cryptographic operations, the evaluation of trust in different tokens and the enforcement of access control security policies.

Stream analysis at the edge of the network is supported in LinkSmart via recently added component - Data-Processing Agent (DPA). It is built upon a Complex Event Processing (CEP) engine and enables to fuse, aggregate, and annotate MQTT or REST events published in a broker, or push into DPA. The DPA is a micro-service which can be use at the cloud, creating multiple instances of it. The creation of a DPA mesh, allows to distribute the load.

2.2.3 OpenIoT

OpenIoT is a full featured IoT Software platform that includes all key features stated at the beginning of this section, visual tools for configuration and management, as well as query formulation and displaying results of discovered services. An overview of the OpenIoT architecture and main components is shown in Figure 12 [25].

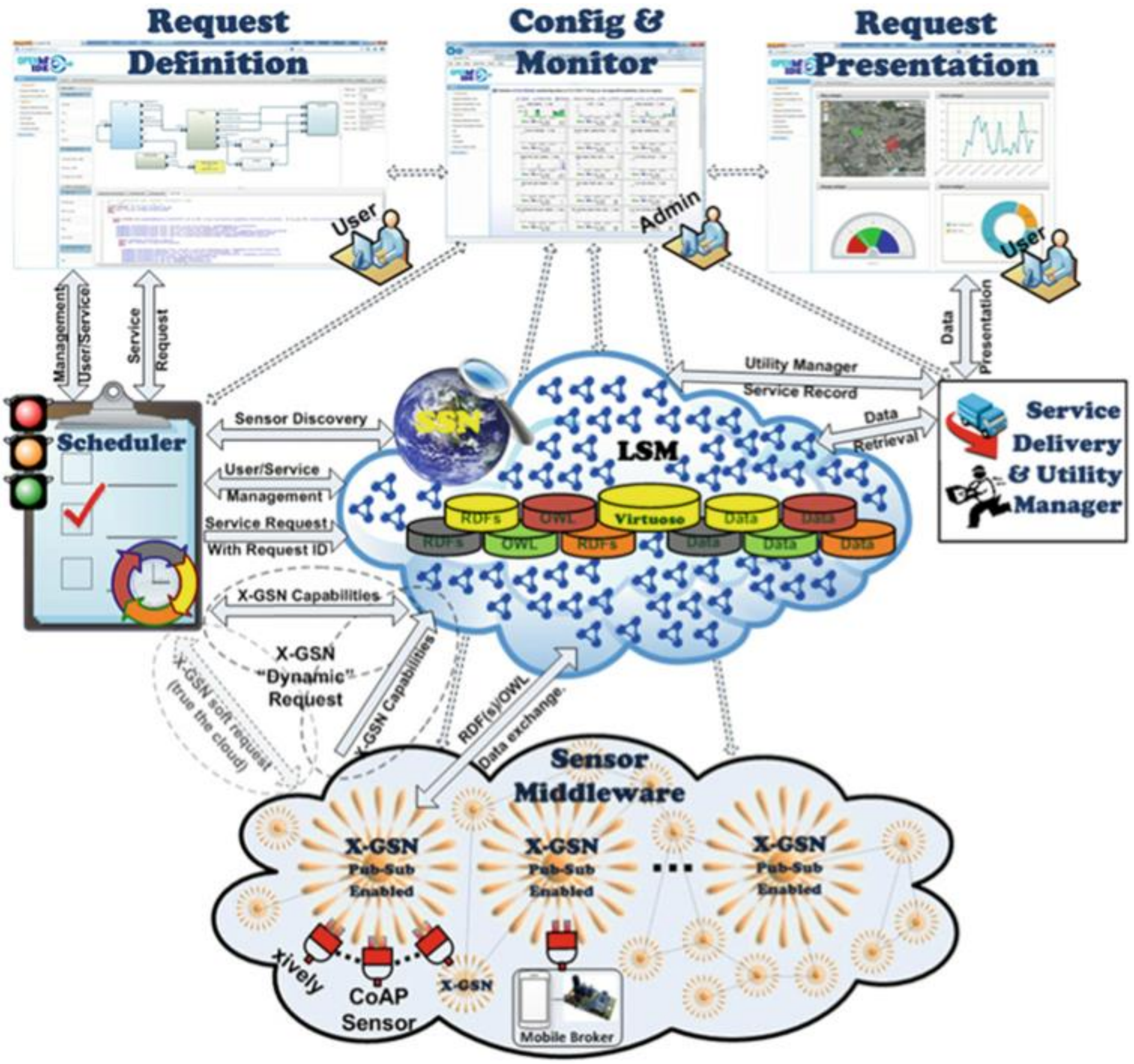


Figure 12: Overview of OpenIoT architecture and main components.

The main elements of the OpenIoT architecture depicted in Figure 12 are:

- The Sensor Middleware – Extended Global Sensor Network (X-GSN) for collecting, filtering and combining data streams from virtual sensors or physical devices. Mobile broker – a publish/subscribe middleware – is used for support of mobile crowd sensing type of application.
- The Cloud Data Storage – Linked Stream Middleware Light (LSM-Light) – cloud DB for storing the data streams together with metadata, used in push-pull style by OpenIoT.
- The Scheduler – process requests of services, discovers sensors and associates data streams.
- The Service Delivery & Utility Manager – combines data streams in order to deliver the requested service (typically expressed as an SPARQL query).
- The Request Definition – component for specification of service requests with GUI interface.
- The Request Presentation – component for visualisation of the outputs of a service.
- The Configuration and Monitoring – support visual management of sensors and services in OpenIoT.

In order to process data from a sensor in OpenIoT, it has to be registered as a virtual sensor through X-GSN within the LSM by posting a semantically annotated representation of its metadata. After the registration corresponding RDF triples are stored in LSM and the sensor is available for discovery and accessing the data. Data access is conveyed by wrappers (via serial port, UDP, HTTP, JDBC…). However virtual sensor can be also aggregation of other virtual sensors or any computation over them.

User management, authentication and authorisation are performed by extended OAuth2.0 enabled Jasig CAS.

OpenIoT IDE supports definition of IoT services without mastering the details of the SPARQL language, discovery of sensors based on location and type, configuration of sensor's metadata, monitoring of IoT services and visualisation of IoT services based on Web2.0 mashups.

2.2.4 FIWARE

FIWARE [26] is an open architecture and operative software (not locked-in to specific vendors) for the creation and delivery of services, related to different areas implemented in the context of the FI-PPP program (Future Internet Public Private Partnership). The goal of the FI-WARE platform is to build an open sustainable ecosystem around public, royalty-free and implementation-driven software platform standards that will ease the development of new Smart Applications in multiple sectors.

FIWARE platform is supported by the FiIWARE community, all people who support FIWARE (users, developers, industry, accelerators, iHubs, OASC, startups & SMEs, cities, stakeholders in the foundation and their employees…) materialised through the FIWARE Foundation, the legal entity to support FIWARE community and the FIWARE OSC, the Open Source Community of persons who develop the FIWARE technologies.

The reference architecture of the FI-WARE platform is structured as presented in Figure 13.

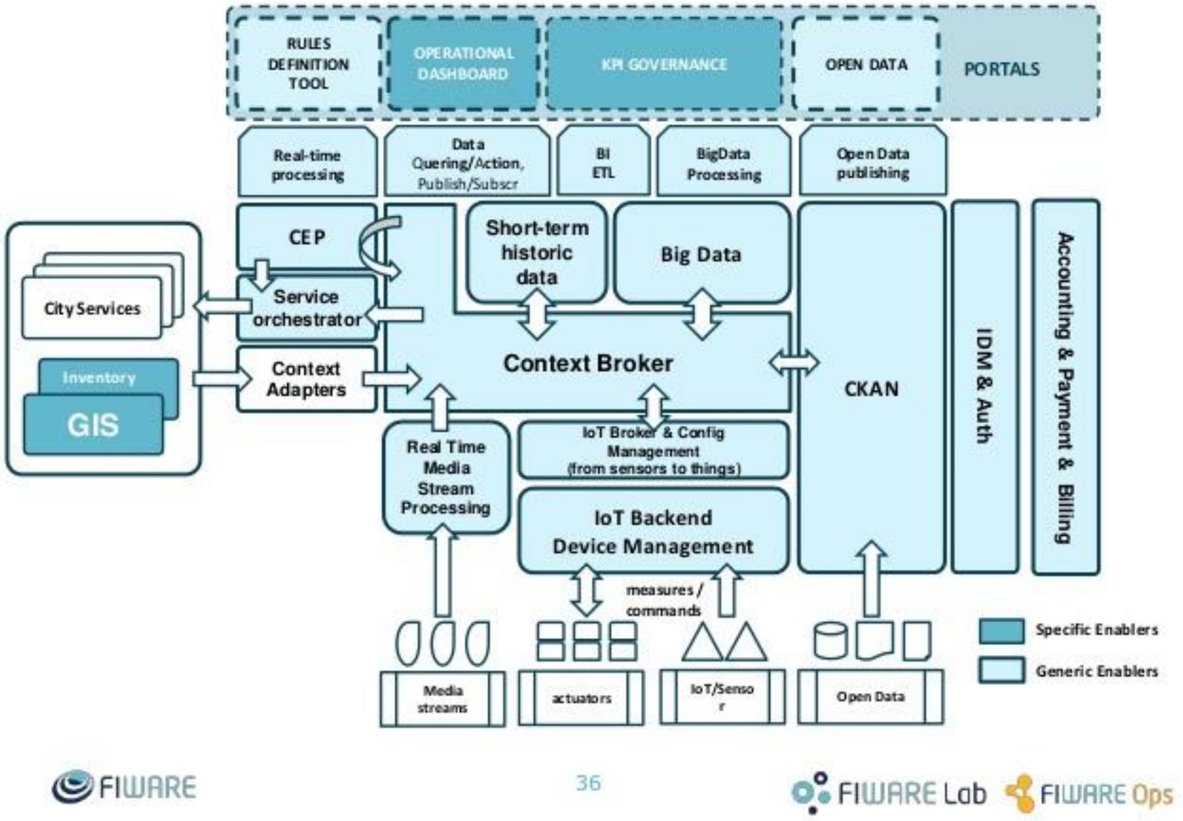


Figure 13: FIWARE Architecture.

The reference architecture of the FI-WARE platform is structured along a number of technical chapters, namely:

- Cloud Hosting
- Data/Context Management
- Internet of Things (IoT) Services Enablement
- Applications/Services Ecosystem and Delivery Framework
- Security
- Interface to Networks and Devices (I2ND)

3 VICINITY Platform/Architecture Standards Requirements

VICINITY standards requirements can be divided into the generic requirements of the platform (e.g. IoT Interoperability and Service Discovery) and the specific requirements of the 'horizontal' domains that rely on it. This section focuses on Platform/Architecture standards requirements. The following section (Section 4) will focus on the requirements of the VICINITY Pilots for standards. A particular concern is privacy (or confidentiality in the case of e-health) which has to be addressed across all domains.

VICINITY Core components such as VICINITY neighbourhood manager, VICINITY Communication Server and Semantic discovery & dynamic configuration agent platform need to be designed, implemented, tested and deployed. Each stage of the life-cycle will follow specific principles of software engineering and common used standards. During design and implementation VICINITY should follow:

- ISO/IEC 30141 20160527 Information technology — Internet of Things Reference Architecture (IoT RA).
- W3C WoT IG, which is looking at IoT platform interoperability.
- ISO/IEC 19501:2005, Information technology -- Open Distributed Processing -- Unified Modeling Language (UML)
- ECSS Space engineer software standards (ECSS-E-ST-40C and family ECS-E-ST-10).

3.1 Cross-domain/cross-vendor IoT Interoperability

Current IoT deployments use a multi-tiered architecture that combines nodes, hubs, and cloud-based services. In the absence of a common systems engineering approach to specify where different types of rules are applied, nodes cannot know where the data they supply will be interpreted, or even that it will be interpreted only once. Contextualizing the data they send will increase the likelihood that it can be interpreted correctly. That contextualization should reference the most primitive possible schema or data model that results in a correct understanding, in order to increase further the chance of correct interpretation and to avoid leakage of unnecessary data about the system to observers.

VICINITY aims to support IoT interoperability by employing a generic IoT ontology based on and extending existing standards (from W3C, ETSI, oneM2M, etc.) to interchange IoT data in a range of standardised and proprietary formats. This support for interoperability will be extended to address the specific requirements of cross-IoT-domain value added services.

VICINITY has a decentralised philosophy that is flexible on the data format used and removes the non-technical interoperability barriers present in centralised solutions.

Key challenges are:

- Ontologies that formalize the meaning of domain data and information models
- Ontology merging, matching and alignment strategies across domains
- Semantic discovery of services, devices, things and their capabilities
- Semantic metadata

Interoperability levels are considered to be [27]:

- Technical Interoperability: is usually associated with hardware/software components, systems and platforms that enable machine-to-machine communication to take place. This kind of interoperability is often centred on (communication) protocols and the infrastructure needed for those protocols to operate.

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

Semantic interoperability will be important at many levels as shown in Figure 14.

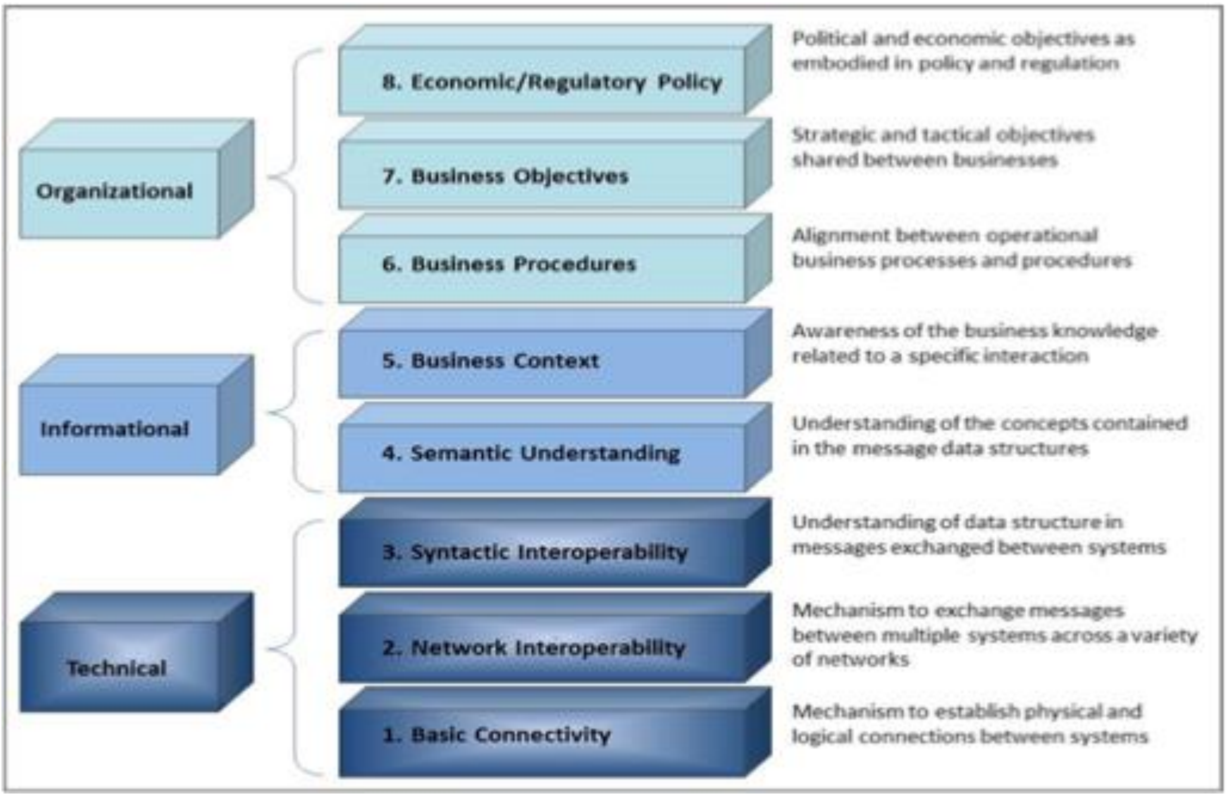

Organizational
Informational
Technical
8. Economic/Regulatory Policy
7. Business Objectives
6. Business Procedures
5. Business Context
4. Semantic Understanding
3. Syntactic Interoperability
2. Network Interoperability
1. Basic Connectivity
Political and economic objectives as embodied in policy and regulation
Strategic and tactical objectives shared between businesses
Alignment between operational business processes and procedures
Awareness of the business knowledge related to a specific interaction
Understanding of the concepts contained in the message data structures
Understanding of data structure in messages exchanged between systems
Mechanism to exchange messages between multiple systems across a variety of networks
Mechanism to establish physical and logical connections between systems

Figure 14: Semantic interoperability is important at many levels

3.2 Semantic Devices, Service Discovery and Dynamic Configuration

VICINITY aims to develop an automatic discovery process of IoT devices using the most adopted semantic descriptions. The VICINITY discovery process will also dynamically update its capabilities based on continuous crawling of existing heterogeneous repositories of devices. The aim is to create a fully automatic process for standardized IoT resources, based on standards supported by the VICINITY discovery module. As soon as a new device descriptor appears in any of the monitored internet based repositories, VICINITY automatically maps it to the VICINITY IoT ontology and from that moment the device becomes known to the VICINITY auto discovery service.

In terms of VICINITY, the dynamic configuration of device means extending the model of device mapped into common VICINITY ontology with information necessary for executing the specific device services, such as retrieving the data or calling actuator functionalities. For this purpose, the part of the VICINITY ontology is the semantic model of services to enable unified way of manipulation with device functionalities. The part of dynamic configuration process is the alignment of service input output properties, such as units of measurement and extension of VICINITY device profiles with information necessary for lookup and matching the devices and their services in terms of functionality or purpose.

This section contains the overview of selected standards for device descriptions, service descriptions will be described in more details in next section.

In the IoT world, there exist plenty of available device description standards. The idea of most of them is based on similar concepts for describing devices, services, functionalities and several profiles (such as vendors or energy profiles). Each standard is created for a specific purpose, so it is very hard to decide for a common standard to build on. However, we provide a list of most common standards for device description, which can be fully or partially reused to build a common VICINITY device ontology.

3.2.1 W3C Semantic Sensor Network ontology

The Semantic Sensor Network ontology (commonly known as "SSN") is an OWL-2 DL ontology for describing sensors and the observations they make of the physical world. SSN is based on the OGC Sensor Web Enablement standards (SensorML and Observations & measurements) and is published in a modular architecture that supports the judicious use of "just enough" ontology for diverse applications, including satellite imagery, large scale scientific monitoring, industrial and household infrastructure, citizen observers, and Web of Things (WoT) [28]. The ten core conceptual modules and key concepts and relations of the SSN ontology are shown in Figure 15.

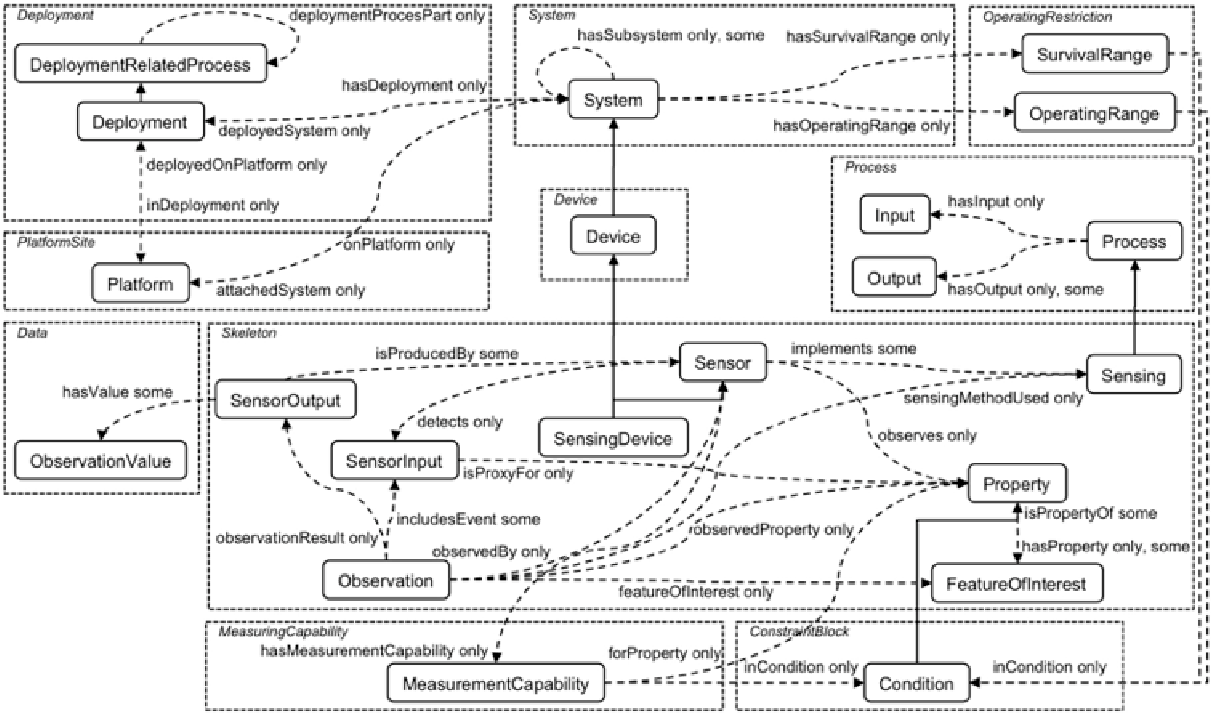


Figure 15: Semantic Sensor Network Ontology

The SSN ontology contains concepts and relations relevant only to sensors, leaving concepts related to other, or multiple, domains to be included from other ontologies when the ontology is used. Doing so makes the ontology single subject and so aims for modularity and reusability. The ontology describes sensors, the accuracy etc. of such sensors, observations and methods used for sensing. Also concepts for operating and survival ranges are included, as these are often part of a given specification for a sensor, along with its performance within those ranges. Finally, a structure for field deployments is included to describe deployment lifetime and sensing purpose of the deployed macro instrument. Modelling of concepts such as units of measurement, locations, hierarchies of sensor types, and feature and property hierarchies are left to other ontologies. The intention was to create core sensor description ontology, which can be easily extended with specific domain concepts.

3.2.2 OGC SensorML: Sensor Model Language

The primary focus of the Sensor Model Language (SensorML) is to provide a robust and semantically-tied means of defining processes and processing components associated with the measurement and post-measurement transformation of observations [29]. This includes sensors and actuators as well as computational processes applied pre- and post-measurement. The main objective is to enable interoperability, first at the syntactic level and later at the semantic level (by using ontologies and semantic mediation), so that sensors and processes can be better understood by machines, utilized automatically in complex workflows, and easily shared between intelligent sensor web nodes. This standard is one of several implementation standards produced under OGC's Sensor Web Enablement (SWE) activity. This standard is a revision of content that was previously integrated in the SensorML version 1.0 standard (OGC 07-000).

SensorML is a means by which sensor systems or processes can make themselves known and discoverable. SensorML provides a rich collection of metadata that can be mined and used for discovery of sensor systems and observation processes. This metadata includes identifiers, classifiers, constraints (time, legal, and security), capabilities, characteristics, contacts, and references, in addition to inputs, outputs, parameters, and system location.

It can provide a complete and unambiguous description of the lineage of an observation, it can describe in detail the process by which an observation happened. The original driver was to enable discovery of sensors distributed over the web, and to execute their services on-demand without a priori knowledge of the sensor or processor characteristics. The self-describing characteristic of SensorML-enabled sensors and processes also supports the development of auto-configuring sensor networks, as well as the development of autonomous sensor networks in which sensors can publish alerts and tasks to which other sensors can subscribe and react. Finally, SensorML provides a mechanism for archiving fundamental parameters and assumptions regarding sensors and processes, so that observations from these systems can still be reprocessed and improved long after the origin mission has ended.

SensorML is currently encoded in XML Schema. However, the models and encoding pattern for SensorML follow Semantic Web concepts of Object-Association-Object. Therefore, SensorML models could easily be encoded for the Semantic Web. In addition, SensorML makes extensive use of soft-typing and linking to online dictionaries for definition of parameters and terms.

3.2.3 SenML: Sensor Markup Language

SenML defines media types for representing simple sensor measurements and device parameters in the Sensor Markup Language (SenML) [30]. Representations are defined in JavaScript Object Notation (JSON), eXtensible Markup Language (XML) and Efficient XML Interchange (EXI), which share the common SenML data model. A simple sensor, such as a temperature sensor, could use this media type in protocols such as HTTP or CoAP to transport the measurements of the sensor or to be configured.

SenML is designed so that processors with very limited capabilities could easily encode a sensor measurement into the media type, while at the same time a server parsing the data could relatively efficiently collect a large number of sensor measurements. There are many types of more complex measurements and measurements that this media type would not be suitable for. A decision was made not to carry most of the metadata about the sensor in this media type to help reduce the size of the data and improve efficiency in decoding. The markup language can be used for a variety of data flow models, most notably data feeds pushed from a sensor to a collector, and the web resource model where the sensor is requested as a resource representation (GET /sensor/temperature).

The main design goal is to be able to send simple sensor measurements in small packets on mesh networks from large numbers of constrained devices.

3.2.4 oneM2M Base Ontology

Ontologies are used in oneM2M to provide syntactic and semantic interoperability of the oneM2M System with external systems [31]. These external systems are expected to be described by ontologies. The only ontology that is specified by oneM2M is the oneM2M Base Ontology formalized in OWL. The oneM2M Base Ontology is the minimal ontology that is required such that other ontologies can be mapped into oneM2M. The core of oneM2M ontology is illustrated in Figure 16.

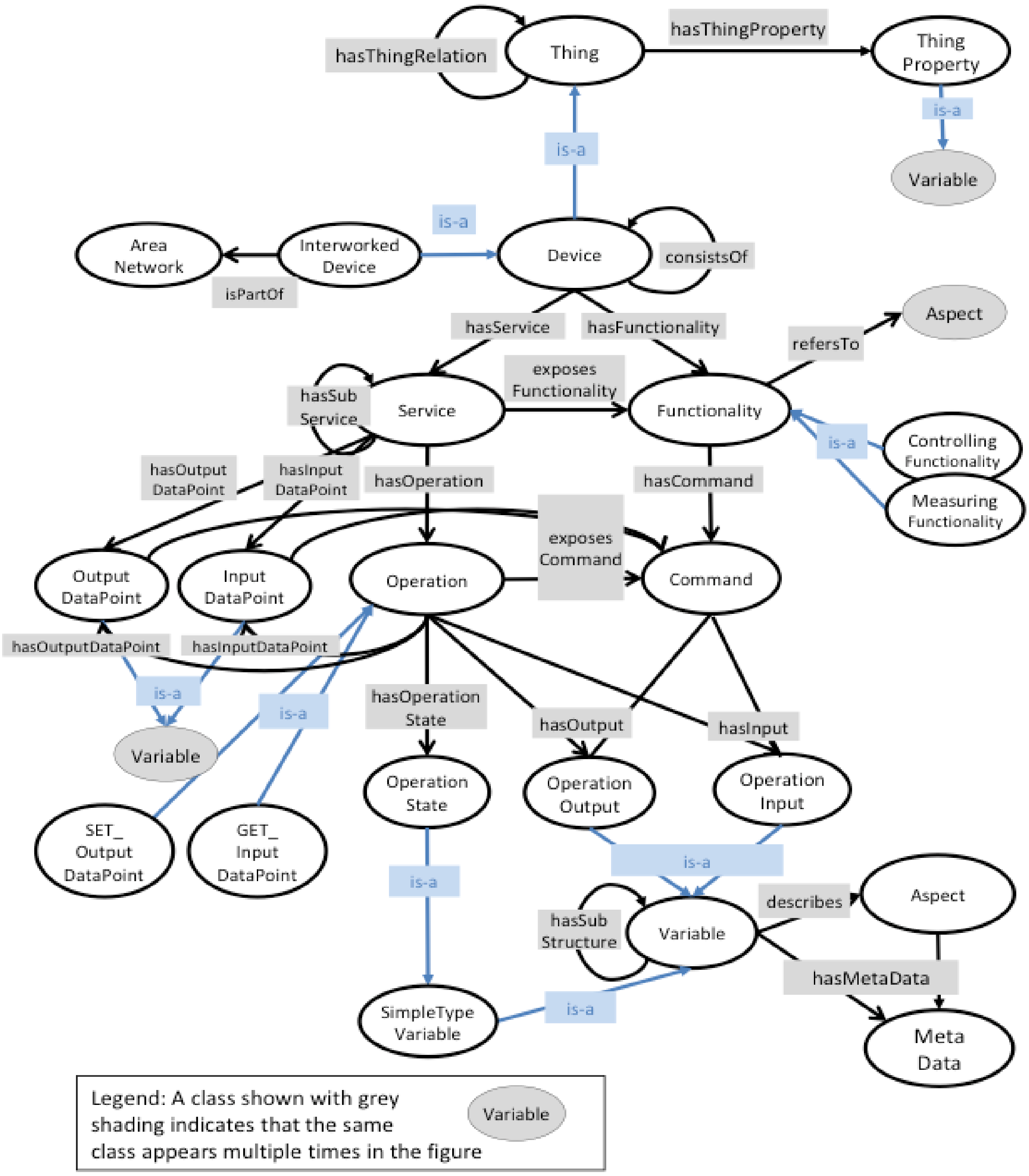


Figure 16: OneM2M Base Ontology.

The Base Ontology has been designed with the intent to provide a minimal number of concepts, relations and restrictions that are necessary for semantic discovery of entities in the oneM2M System. To make such entities discoverable in the oneM2M System they need to be semantically described as classes (concepts) in a - technology/vendor/other-standard specific - ontology and these classes (concepts) need to be related to some classes of the Base Ontology as sub-classes.

Additionally, the Base Ontology enables non-oneM2M technologies to build derived ontologies that describe the data model of the non-oneM2M technology for the purpose of interworking with the oneM2M System.

The Base Ontology only contains Classes and Properties but not instances because the Base Ontology and derived ontologies are used in oneM2M to only provide a semantic description of the entities they contain.

Instantiation (i.e. data of individual entities represented in the oneM2M System - e.g. devices, things, etc.) is done via oneM2M resources.

3.2.5 SAREF: Smart Appliances REFerence ontology

The Smart Appliances REFerence (SAREF) ontology is a shared model that facilitates the matching of existing assets (standards/protocols/datamodels/etc.) in the smart appliances domain [32]. The SAREF ontology provides building blocks that allow separation and recombination of different parts of the ontology depending on specific needs.

The starting point of SAREF is the concept of Device (e.g., a switch). Devices are tangible objects designed to accomplish one or more functions in households, common public buildings or offices. The SAREF ontology offers a lists of basic functions that can be eventually combined in order to have more complex functions in a single device. For example, a switch offers an actuating function of type "switching on/off". Each function has some associated commands, which can also be picked up as building blocks from a list. For example, the "switching on/off" is associated with the commands "switch on", "switch off" and "toggle". Depending on the function(s) it accomplishes, a device can be found in some corresponding states that are also listed as building blocks.

A Device offers a Service, which is a representation of a Function to a network that makes the function discoverable, registerable and remotely controllable by other devices in the network. A Service can represent one or more functions. A Service is offered by a device that wants (a certain set of) its function(s) to be discoverable, registerable, remotely controllable by other devices in the network. A Service must specify the device that is offering the service, the function(s) to be represented, and the (input and output) parameters necessary to operate the service. A Device in the SAREF ontology is also characterized by an (Energy/Power) Profile that can be used to optimize the energy efficiency in a home or office that are part of a building.

3.3 From Ontologies of Things to Ontologies of Services

VICINITY aims to connect different isolated IoT infrastructures in order to create added value from them. However, such value creation depends on the effective collaboration between heterogeneous networks of cross-domain devices and services.

As discussed above, collaboration between different IoT infrastructures requires achieving semantic interoperability between them, so devices and data can be discovered, and data can be interchanged and understood among the different infrastructures.

This requires, on the one hand, to enhance IoT data with metadata that describes its context (source, time, location, etc.) and, on the other hand, to represent such data (and metadata) using ontologies that express the shared meaning of the data and ensure data consistency.

In order to ensure the common way of lookup and matching of devices and their services, the VICINITY ontology must contain the rich model of services enabling intelligent service discovery and execution. These concepts are based on well-known SOA (Service Oriented Architecture) approach. In SOA, distributed information systems enable loose coupling of system elements, i.e. various functional modules that provide and/or consume shared or private information resources, in a transparent way, by means of standardised service interfaces. The core concepts, which should be taken into account when designing the semantic service models are:

- Service publication – service descriptions are created in a suitable format and are published according to pre-defined standards in well-known locations;
- Service discovery – information retrieval techniques are employed on the published service descriptions;
- Service selection – results of the discovery process are filtered according to the specified query parameters;
- Service binding – the interface and transport protocol of a service is specified and the service is ready to be executed.

Again there is plenty of several semantic service descriptions, however, except very specific domain parts of models, the most of them are based on common, already older, standards, listed below.

3.3.1 OWL-S: Semantic Markup for Web Services

The Semantic Markup for Web Services (OWL-S) is the OWL ontology for semantic description of web services [33]. The structure of OWL-S consists of a service profile for service discovery, a process model which supports composition of services, and a service grounding that associates profile and process concepts with the underlying service interfaces. Currently, OWL-S is available in Version 1.2. The class ServiceProfile of the OWL-S ontology provides a superclass of every type of high-level description of the service. It defines functional properties that describe IOPEs of a service, as well as non-functional properties that describe semi-structured human-readable information for service discovery, e.g. service name, description and parameters which incorporates further requirements on the service capabilities (e.g. security, quality-of-service, geographical scope, etc.). The class Service model specifies ways of operating the service in a workflow structure with other services. The service is viewed as a process, which defines the functional properties of the service (IOPEs) together with details of its constituent processes (if the service is a composite service). Functional properties of the service model can be shared with the service profile. Interactions between services are represented by service grounding. It enables execution of the Web Service by binding the abstract concepts of the OWL-S profile and process model to concrete message formats and communication protocols. Although different message specifications are supported by OWL-S, the widely accepted WSDL is preferred as an initial grounding mechanism.

3.3.2 The Semantic Annotations for WSDL and XML Schema: SAWSDL

The Semantic Annotations for WSDL and XML Schema (SAWSDL) recommendation [34] defines a set of extension attributes for WSDL, which allows an insertion of semantic descriptions for web services. While the syntactic descriptions of WSDL provide information about the structure of input and output messages of an interface and about how to invoke the service, semantic extension is needed to describe what a web service actually does. The SAWSDL specification defines how semantic annotation is accomplished using references to semantic models, e.g. ontologies. It provides mechanisms by which ontology concepts, typically defined outside the WSDL document, can be referenced from within WSDL and XML Schema components using semantic annotations. The annotation mechanism of SAWSDL uses the abstract definition of services, which is represented in WSDL by Element Declaration, Type Definition, and Interface components. Such a semantic annotation of abstract part of the service definition consequently enables dynamic discovery, composition and invocation of services. The extension attributes defined by SAWSDL are as follows:

- the modelReference attribute specifies the association between a WSDL or XML Schema component and a concept in some semantic model;
- the liftingSchemaMapping and loweringSchemaMapping extension attributes are added to XML Schema element declarations and type definitions for specifying mappings between semantic data and XML.

Multiple semantic annotations are allowed for a single WSDL element in service descriptions. Both schema mappings and model references can contain multiple pointers - URIs that typically refer to concepts described in an external ontology. Multiple schema mappings are interpreted as alternatives whereas multiple model references are all applied in parallel. SAWSDL does not specify any other relationship between them.

3.3.3 The Web Service Modelling Ontology: WSMO

The Web Service Modelling Ontology (WSMO) is a conceptual model that was specifically developed for describing semantic web services [35]. The underlying ontological specification of WSMO consists of four major components - ontologies, goals, web services, and mediators. Ontologies provide an agreed common terminology, a formal semantics that can be used by all other components. WSMO specifies the following constituents as a part of the description of ontology: concepts, relations, functions, axioms, together with instances of concepts and relations, as well as non-functional properties, imported ontologies, and used mediators. Goals specify objectives that a client might have when consulting a web service, i.e. functionalities that a web service should provide from the user perspective. The Goal element is characterized by a set of non-functional properties, imported ontologies, used mediators, the requested capability and the requested WSDL interface. The Web Service elements are described by non-functional properties, references to imported ontologies, used mediators, and the behavioural aspects of web services that are represented by the capability and interface properties. The capability of a web service defines its functionality in terms of preconditions, postconditions, assumptions and effects, which are expressed by a set of axioms and shared variables. By means of the capability property, a web service may be linked to certain goals that are solved by the web service by means of referenced mediators. The interface of a web service provides further information on how the service functionality is achieved. It describes the behaviour of the service for the client's point of view (i.e. service choreography) as well as the means of achieving overall functionality of the service in terms of cooperation with other services (service orchestration).

Mediators represent the elements that enable overcoming structural, semantic or conceptual mismatches that appear between the components that build up a WSMO description.

All WSMO components are formalized using the Web Service Modelling Language (WSML), which is based on the description logic, first-order logic and logic programming formalisms [36]. The WSMO framework is supported by the Web Service Modelling eXecution environment (WSMX), which serves as a reference implementation for WSMO [37].

3.4 Standard Ontologies

VICINITY aims to connect different isolated IoT infrastructures in order to create added value from them. However, such value creation depends on the effective collaboration between heterogeneous networks of cross-domain devices and services.

As discussed above, collaboration between different IoT infrastructures requires achieving semantic interoperability between them, so devices and data can be discovered, and data can be interchanged and understood among the different infrastructures.

This requires, on the one hand, to enhance IoT data with metadata that describes its context (source, time, location, etc.) and, on the other hand, to represent such data (and metadata) using ontologies that express the shared meaning of the data and ensure data consistency.

Nowadays, with the current proliferation of IoT data, it is essential to have open standard ontologies that can be reused across different domains.

VICINITY aims to go beyond the modelling of “Things” (i.e., devices) in order to provide a common ontology model that enables the representation of rich data in IoT neighbourhoods that enables the development of value added services. Such an ontology model will be based on existing standards (from W3C, OGC, ETSI, oneM2M, etc.) and will provide feedback in order to enhance them.

This relies on the following standards:

- W3C Semantic Sensor Network (SSN) ontology, developed in the W3C Semantic Sensor Networks Incubator Group and currently being standardised in the W3C Spatial Data Web WG.
- Smart Appliances REFerence ontology (SAREF) [38], developed by TNO under a contract with the EC and standardised by ETSI in ETSI TS 103 264 Smart Appliances Common Ontology and oneM2M Mapping.
- oneM2M base ontology, developed by the oneM2M partnership project.

The W3C OWL standard is the formal Knowledge Representation language that is accepted ‘universally’ for implementing ontologies. There are many similar languages such as ISO 24707 but these do not need to be covered here.

3.5 Value-added Services in IoT

VICINITY will exploit its inherent ubiquitous interoperability to serve as a testbed for developing cross-domain value-added services of various types. Underlying semantic knowledge mechanisms and the applied concept of social networking will enable VICINITY to demonstrate advances in IoT services interoperability that will combine business intelligence with energy consumption monitoring. Artificial Intelligence (AI) algorithms for data mining, prediction and optimization will also be used to provide smart parking and eHealth services.

This relies on the following standards:

- **ISO/IEC 20005:2013** - Information technology -- Sensor networks -- Services and interfaces supporting collaborative information processing in intelligent sensor networks
- **ISO 14813-1:2015** – Intelligent transport systems -- Reference model architecture(s) for the ITS sector -- Part 1: ITS service domains, service groups and services

3.6 Open Smart Appliances

VICINITY will enable a smarter household in terms of a more efficient and more open use of the information and services provided by smart appliances. By gathering data from different household (smart) appliances, in particular from sensors that are incorporated in them, energy efficiency will be improved. VICINITY will go beyond this to create ways to open the data and services of the smart appliances to independent service operators. The availability of the data from smart appliances will pave the way to new services in other domains such as security, e-health and transport that will have an impact on individuals and the community as a whole.

The standards that Smart Appliances will rely on will include:

- Smart Appliances REFerence ontology (SAREF) [32] developed by TNO under a contract with the EC and standardised by ETSI, while CERTH has also been an active member on the ongoing activities organised by TNO.
- ETSI TS 103 267 Smart Appliances; Communication Framework.
- ETSI TS 103 264 Smart Appliances Common Ontology and oneM2M Mapping.

Smart appliances will be brought into the project by VICINITY partner Gorenje who will incorporate proprietary solutions relevant to the embedded development needs [39] However, standardized web technologies will be used to connect Gorenje's smart appliances with the VICINITY platform via an appropriate API. The services, such as discovery, identification and appliances' profiles, will provide an efficient way to handle these smart appliances.

3.7 Security

IoT will not create an improvement in peoples' lives unless their concerns over accessibility, data protection, security and privacy are addressed. Standards are critical to these issues as well as for interoperability.

Topics relevant to Security include Identity Management, Anonymity and Pseudonymity, Credentials and Attributes and Access Management.

Adequate security for the IoT should consider the following standards:

- ITU-T Security in Telecommunications and Information Technology: An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications;
- ITU-T Recommendation E.408: Telecommunication networks security requirements;
- EN 61508 Functional safety;
- ISO 9160 Data encipherment -- Physical layer interoperability requirements;
- IEEE 802.11 Security of wireless communication networks;
- IETF RFC 2818 HTTP Over TLS [40];

End-to-end should be included in the VICINITY communications layer in order to provide adequate security for information in the IoT. However, a key issue is the difficulty of achieving sub-mS end-to-end-response times for exchange of data if encryption and decryption are to be used by IoT devices, especially if using a Trusted Third Party (TTP) architecture. This is not possible using current technologies.

Organizations working on IoT security include:

- Cloud Security Alliance (CSA)
- ETSI TC Cyber

- ISO/IEC JTC 1/WG 10 on IoT
- ITU-T SG 20

VICINITY should steer the development of lightweight end-to-end encryption for the IoT in these bodies. The Chair of ETSI TC Cyber is a member of the VICINITY Stakeholder Advisory Board (SAB) and will provide advice to VICINITY on the best way to proceed.

3.8 Privacy

Privacy is a primary concern for the IoT. While it is intended to greatly benefit consumers and improve quality of life for society at large, it also introduces new types of privacy threats and challenges including:

a) Misuse of personal data due to ease of data flow and lack of transparency & control.
b) Occurrence of an unwanted action which could cause physical harm, loss or theft of property. For example, a hacker could tamper with a sensor attached to a device such as a car garage door, activate it and allow an intruder into the victim's house.
c) A wanted action not occurring which could lead to safety concerns due to a physical action triggered remotely by a genuine owner not getting executed. This could result in an accident, e.g., if an owner switches off a kitchen oven from a smartphone which doesn't actually switch off, possibly due to a sensor not working or it switching off a neighbour's oven instead.
d) When more than one individual is associated with a device, whose consent is needed to process the data,
e) How do we establish the identity of a device and how is it changed when the owner changes?
f) An authentication risk, since the device is often not in physical proximity to individual.
g) The complexity of the IoT architecture, with multiple data controllers and processors, which makes it more difficult to pinpoint the source of any privacy breaches.

VICINITY should consider standards from ISO/IEC JTC1/SC27/WG5 "Identity Management and Privacy Technologies" which covers the development and maintenance of standards and guidelines addressing security aspects of identity management, biometrics and the protection of personal data.

Organizations working on Privacy in the IoT include:

- AIOTI WG3
- Article 29 WP study on IoT

Topics relevant to Privacy include a privacy framework, a privacy reference architecture, privacy infrastructures, privacy impact assessment and specific privacy enhancing technologies (PETs).

4 VICINITY Pilot Standards Requirements

This section comprises a list of standards considered in each of the pilot site locations in Greece, Norway and Portugal. For detailed descriptions of pilot site locations please see Deliverable D1.3 - Report on pilot sites and operational requirements.

4.1 Pilot 1: Smart Grid and Parking

Smart Grid and Parking will be implemented in Norway to demonstrate the interconnection of smart objects under a 'virtual neighbourhood' of intelligent buildings, smart parking and EV charging. The virtual neighbourhood enables environment efficiency of intelligent buildings through added-value services. These improve energy efficiency through demand management of EV charging and smart parking.

These functionalities will rely on the following standards, for deeper analysis of Building domain standards see Annex A: Building domain standard considerations:

- CEN TS 16157-1, 2, 3, 6 Intelligent transport systems - DATEX II data exchange specifications for traffic management and information standards family;
- prEN 12414 Vehicle parking control equipment — Requirements on a parking terminal
- ISO CD 13184-2 Intelligent transport systems (ITS) — Guidance protocol via personal ITS station for advisory safety systems — Part 2: Road guidance protocol (RGP) requirements and specification
- EN 62628 Guidance on software aspects of dependability
- EN 55022 Information technology equipment – Radio disturbance characteristics – Limits and methods of measurement
- ETSI EN 300 220 Electromagnetic compatibility and Radio spectrum Matters (ERM); Short range devices; Technical characteristics and test methods for radio equipment to be used in the 25 MHz to 1 000 MHz frequency range with power levels ranging up to 500 mW; Part 1: Parameters intended for regulatory purposes;
- ISO TC 163/SC 2/WG 10 is focused on (CEN TC89/WG4/N284) Energy performance of buildings — Calculation of energy use for space heating and cooling

Technical requirements that must be included in the specifications for the equipment include:

- EN 62628 Guidance on software aspects of dependability
- EN 55022 EMC requirements
- ETSI EN 300 220 EMC, radio spectrum matters (ERM) description
- ISO/IEC 20922:2016, Information technology - Message Queuing Telemetry Transport (MQTT);

4.2 Pilot 2: Smart Energy Neighbourhood

Smart Energy Neighbourhood will be implemented in Portugal to look at the management of a community-scale smart energy system and municipal buildings in one virtual neighborhood. In virtual neighborhood added value services should focus health, energy and building domain thorough demand response, energy storage, integration of renewables and leverage of equipment to provide services between domains. Added value service such max sun exposure information based on meteorology station of Solar Park should be provided to municipality citizens to reduce health risks. Environment quality (EQ) service should be provided for building management and visitors. EQ services will consider weather forecasts, building occupancy, energy consumption for Near Zero Energy Buildings such as SolarLab and municipal buildings such as School, Swimming pools.

The pilot follows the standards approach of the SmartGrids European Technology Platform [41]. An overview of the current standards efforts relevant to M2M communication in the Smart Grid is shown in Figure 17 [42]. Major focuses of activity are circled in red. Arrows represent links where information is passed between the SDOs.

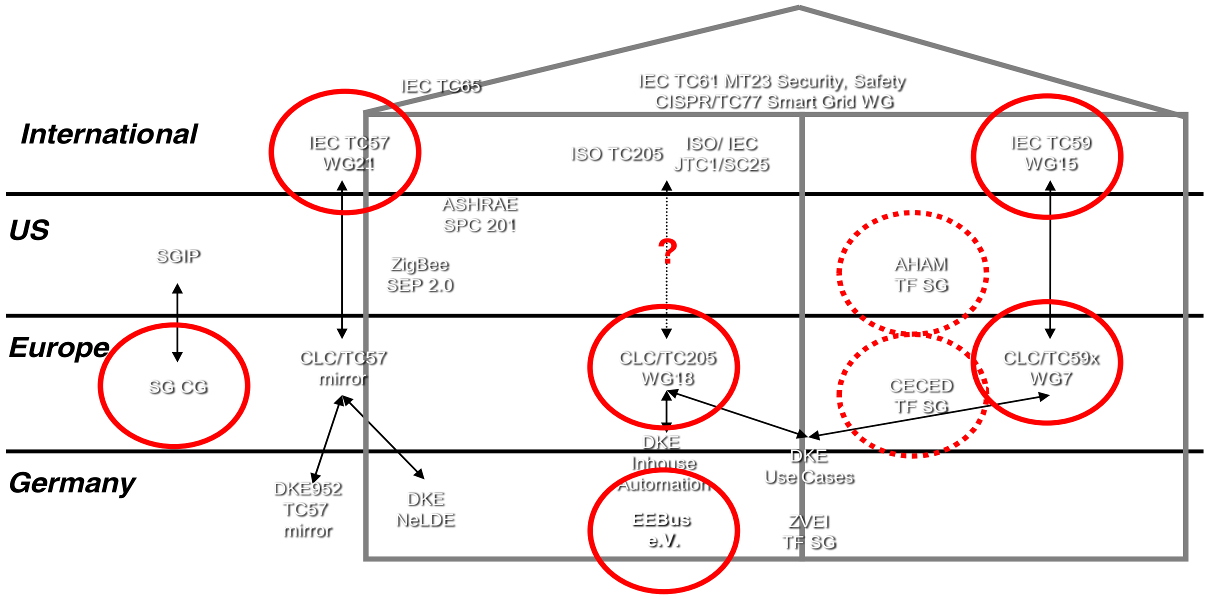


Figure 17: Ongoing standardization initiatives for M2M communication in the Smart Grid.

Specific standards required for the pilot include:

- IEC 61215 (for Crystalline Silicon Modules).
- IEC 61730 (Photovoltaic (PV) module safety qualification - Part 1: Requirements for construction).
- IEC 62109-1,2,3: Safety of power converters for use in PV power systems.

These standards are sufficient as they stand and no modifications are required for use by VICINITY.

Moreover, the Universal Smart Energy (USEF) Framework [43] is potentially relevant to VICINITY as a standards initiative on smart interconnected energy. VICINITY partner ENERCOUTIM should keep a watching brief on USEF and identify the implications for VICINITY.

4.3 Pilot 3: eHealth at Home

EHealth at Home will be implemented in Greece to demonstrate interoperability in the health and building domains in the virtual neighbourhood of a household. Added value services will focus improvement of health assistance for senior citizens and the wellbeing of citizens based on their health status, environment where they live and lifestyle. Moreover, value-added services will include the detection of abnormal events based on data from the building monitoring system and devices. Therefore, typical building sensors will further be of interest in the implementation of this pilot as for the Smart Grid and Parking pilot.

Current standards on which data and information exchange for Pilot 3 will rely include:

- Integrating the Healthcare Enterprise (IHE) Profiles [44];
- Health Level 7 International (HL7) Standards [45];
- The DICOM Standard [46];
- Continua Health Alliance [47].

The main focus will be on IHE, HL7 and Continua. A further series of standards that may need to be considered is ITU-T H.810 Series H: Audiovisual and Multimedia Systems: Interoperability Design Guidelines for Personal health systems. These standards are mature and sufficient as they stand so that modifications should not be necessary for use by VICINITY.

5 Relevant Standards Bodies

There are already a variety of standards and proprietary platforms for the IoT. At the communication level there are a limited number of standards, including WiFi and ZigBee, and so exchanging data between IoT devices is not a problem. The problem is the discovery and classification of services and the communication at the semantic layer that is summarized under the term Machine to Machine communication (M2M). Achieving interoperability and establishing services at this level is more challenging and requires semantic knowledge from different domains and the ability to discover and classify services of things in general. This is difficult to standardize as it changes rapidly and is dependent on particular applications, locations and use cases.

The Alliance for Internet of Things Innovation (AIOTI) has identified a huge range of standards bodies, fora and consortia that are relevant to IoT. An overview is shown in Figure 18 [27].

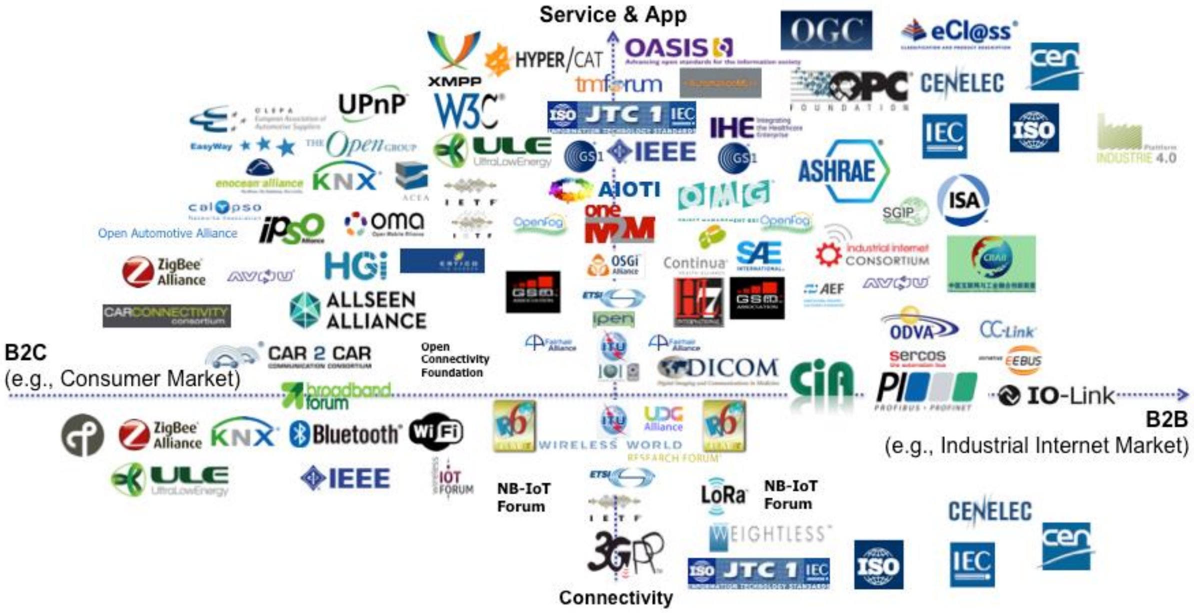


Figure 18: IoT SDOs and Alliances Landscape (Technology and Marketing Dimensions)

The mapping of the VICINITY domains to these IoT standards bodies is shown in Figure 19 [27]. The most relevant bodies are identified and their relevance described later in this section.

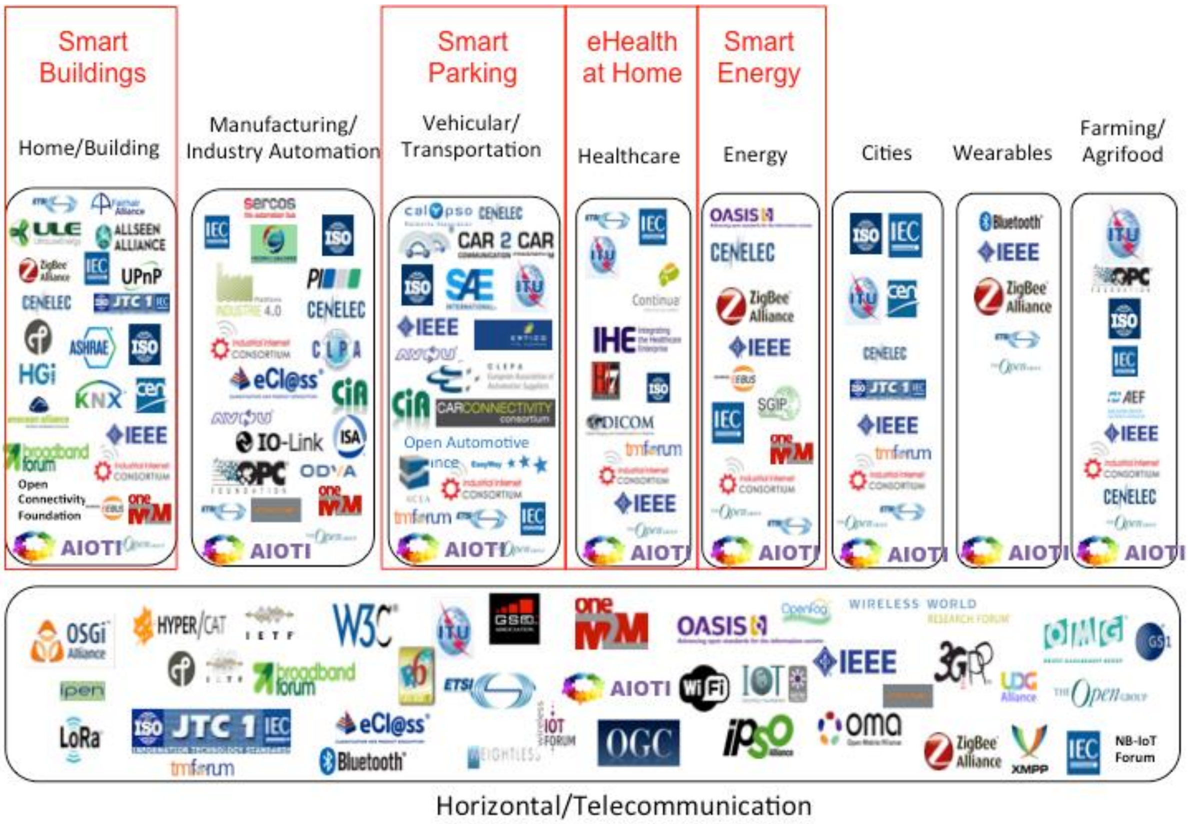


Figure 19: Mapping of VICINITY Domains to IoT SDOs and Alliances Landscape Vertical and Horizontal Domains

The question for all of the standards, either existing or being developed, is can VICINITY use them as they are or does VICINITY need to extend or modify them in order to be able to use them effectively?

5.1 Alliance for Internet of Things Innovation (AIOTI)

AIOTI was set up by the EC in early 2015 in an attempt to generate a consensus on the standards needed to deploy the IoT globally. AIOTI currently has the WGs listed below. The WGs considered most important to VICINITY and its pilot domains are highlighted in bold:

- WG 1: IoT European research cluster
- WG 2: Innovation Ecosystems
- **WG 3: IoT Standardisation (including Privacy)**
- **WG 4: Policy issues**
- **WG 5: Smart living environment for ageing well**
- WG 6: Smart Farming and food security
- **WG 7: Wearables**
- **WG 8: Smart Cities**
- **WG 9: Smart Mobility**
- WG 10: Smart Environment (smart water management)
- WG 11: Smart Manufacturing
- **WG12: Smart Buildings and Architecture**
- **WG13: Smart Energy**

These WGs are not themselves developing standards but will influence the standards and platforms that are eventually adopted for the IoT. Therefore, it would be useful for VICINITY to participate and try to influence these. Not all of the WGs are relevant to VICINITY, but it would be beneficial to participate in at least WG3, WG4 (especially for Privacy), WG5, WG7 (because eHealth sensors will be worn), WG8, WG9 (including ITS and smart parking), WG12: and WG13. Most AIOTI meetings are held remotely using a collaboration tool such as GTM. Face-to-Face meetings and General Assemblies are held infrequently.

AIOTI has recently changed its constitution to become a company registered under Belgian law and has become a membership-based organisation. Partners such as ATOS, CAL, HITS and UPM, who are already members, should represent VICINITY in AIOTI.

5.2 AllSeen Alliance

The AllSeen Alliance [48] is a cross-industry consortium dedicated to enabling the interoperability of billions of devices, services and apps that comprise the IoT. It has developed AllJoyn which is an open source software framework that makes it easy for devices and apps to discover and communicate with each other. Developers can write applications for interoperability regardless of transport layer, manufacturer, and without the need for Internet access. The software has been and will continue to be openly available for developers to download, and runs on popular platforms such as Linux and Linux-based Android, iOS, and Windows, including many other lightweight real-time operating systems.

5.3 AVnu Alliance

The Avnu Alliance is creating an interoperable ecosystem servicing the precise timing and low latency requirements of diverse applications using open standards through certification. This has developed the AVB/TSN standard.

Joining the Avnu Alliance would give VICINITY the opportunity to collaborate in the development of an ecosystem of interoperable IoT devices.

5.4 British Standards Institute (BSI)

The British Standards Institute (BSI) is relevant to IoT because it developed the first three Smart Cities standards:

- PAS 180 Smart cities. Vocabulary.
- PAS 181 Smart city framework.
- PAS 182 Smart city concept model.
- PAS 212 HyperCat
- EPL 278 Intelligent Transport Systems

BSI has developed PAS 212 [49] based on the specification from the HyperCat consortium. This will also be contributed to ISO. Use of the standard facilitates the representation and exposure of IoT data hub catalogues over standard web technologies. This will improve data discoverability and interoperability, allowing a server to provide a set of resources identified by Uniform Resource Identifiers (URIs) to a client, each with a set of semantic annotations. As it offers a repository of available resources (nodes, sensors) it might be useful to help in 4.2, semantic devices, service discovery.

BSI has developed set of standards for Social Alarms namely: BS EN50134-1 2002, BS EN 50134-2 2000, BS EN 50134-3 2012, BS EN 50134-5 2004, BS TS 50134-7 2003.

Participation in BSI is typically via a committee or commission set up to meet a specific requirement for a new standard. BSI experts are principally involved in the drafting process. British standards may subsequently become part of an international standard such as ETSI which then prevails.

5.5 European Committee of Domestic Equipment Manufacturers (CECED)

The European Committee of Domestic Equipment Manufacturers (CECED) [50] is a trade association based in Brussels for the European home appliance industry. It promotes product innovation while reducing the environmental impact of appliances. CECED members produce the following type of appliances:

- Large appliances such as refrigerators, freezers, ovens, dishwashers, washing machines and dryers;
- Small appliances such as vacuum cleaners, irons, toasters and toothbrushes;
- Heating, ventilation and air conditioning appliances such as air conditioners, heat pumps and local space heaters.

Gorenje has a delegate in CECED but only monitors activities relevant to connectivity regulation. Involvement was greater in the run-up to the introduction of the AIS specification.

Gorenje should maintain participation in CECED and try to ensure that standards and specifications developed by them should align with VICINITY requirements.

5.6 European Committee for Standardization (CEN)

CEN is one of the three European Standards organisations (ESOs) formally recognised by the EC as providing European Standards (ENs). Participation is normally only possible through accreditation by a National Standards Organisations (NSO). The full list of CEN Technical Committees (TCs) is given in [51].

5.6.1 TC 204 Medical Devices

CEN TC 204 covers Medical Devices which is relevant to the VICINITY eHealth at Home pilot. It is not clear whether anything needs to be changed to meet this needs of this pilot, and this will be clarified in discussions during ISO/IEC JTC1 in Lillehammer, Norway, in November 2016.

5.6.2 TC 247 Building Automation, Controls and Building Management

CEN TC 247 covers Technical Building Management, Automation & Control. Many of the standards are relevant to the VICINITY Smart Energy Neighbourhood pilot.

5.6.3 TC 251 Health Informatics

CEN TC 251 covers Health Informatics which is relevant to the VICINITY eHealth at Home pilot. HITS (on behalf of VICINITY) should contribute to and test the following standards:

- ISO/FDIS 25237:2016 Health informatics – Pseudonymization
- ISO/IEEE 11073: Health Informatics: Personal health device communication: Device specialization.
- CEN-TC251_N2016076 New Work Item proposal on Health and Wellness apps.

- prEN/ISO/FV 27799 - Health informatics - Information security management in health using ISO/IEC 27002 (ISO/FDIS 27799:2016).

ISO/TC215 (CEN TC251) WG 2: System and device interoperability will next meet in Lillehammer, Norway in November 2016.

5.6.4 TC 278 Intelligent Transport Systems

CEN TC 278 is heavily integrated with ISO TC 204 and covers Transport Telematics and Traffic, which may be relevant to the Smart Grid and Parking pilot.

It is not clear whether VICINITY needs to influence TC 278. They have not started to look at IoT in Transport yet as they do not see connected vehicles as part of the IoT and so do not see the need for open communications except to support specific applications. However, VICINITY participation could encourage them to do so and to steer them towards a more open future in a direction beneficial to VICINITY objectives.

5.6.5 CEN/CLC/ETSI SSCC-CG

The Smart and Sustainable Cities and Communities Coordination Group (SSCC-CG) is a joint coordination group between the three ESOs: CEN, CENELEC and ETSI. It also involves European NSOs and consumer representation bodies such as the European Association for the Co-ordination of Consumer Representation in Standardisation (ANEC) and the European Environmental Citizens Organisation for Standardisation (ECOS).

VICINITY is already represented in SSCC-CG by Keith Dickerson in his role of Smart Cities strategic champion on the ETSI Board.

5.7 European Committee for Electrotechnical Standardization (CENELEC)

CENELEC is also one of the three ESOs formally recognised by the EC as providing European Standards (ENs). Participation is normally only possible through accreditation by an NSO.

The following standards are relevant to smart appliances in VICINITY:

- CENELEC EN 50523-1:2009: Household Appliances Interworking – Part 1: Functional Specification.
- CENELEC EN50523-2:2009: Household Appliances Interworking -- Part 2: Data structures.

CENELEC TC 205 covers Home and Building Electronic Systems (HBES), which may be relevant to the VICINITY Smart Energy Neighbourhood pilot. EN 50090 is the series of European standards for home and building control.

5.8 Continua Health Alliance

The Continua Health Alliance [52] addresses Personal Connected Health and is required for the VICINITY eHealth at Home pilot. Continua currently includes more than 110 industry leading companies and healthcare organizations worldwide. Implementations of Continua specifications in the upcoming area of welfare technologies are popular with European Governments and interest from vendors is growing.

The Continua Health Alliance standard addresses the fundamentals of data exchange between medical devices [53]. Pilot partner GNOMON is already utilizing certified and branded Continua-enabled products in currently implemented eHealth projects, providing the end-users with increased assurance of interoperability between devices and enabling them to easily share information with caregivers and service providers.

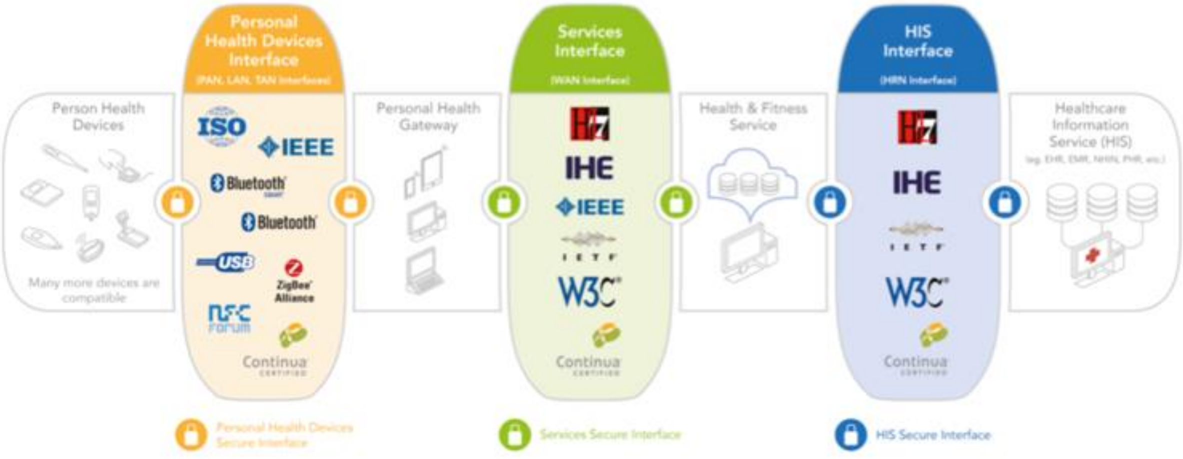


Figure 20: High Level Architecture for Connected E-health Devices.

Continua Design Guidelines provide a flexible implementation framework for authentic interoperability, containing references to the standards and specifications that Continua selected for ensuring interoperability of devices. Some of the standards selected are:

- Bluetooth for wireless and USB for wired device connection,
- ISO/IEEE 11073 Personal Health Data (PHD) Standards
- The IHE (originally IETF) External Data Representation (XDR) standard for the exchange of clinical documents between healthcare enterprises

Continua could provide VICINITY with a standardised way of obtaining information from medical devices although more work would be needed to determine the protocols that would be used.

VICINITY should put an emphasis on Continua since at least Scandinavian governments will require these standards in their procurements. GNOMON should participate in Continua to ensure the approach and resulting specifications are aligned with VICINITY requirements.

5.9 ISO TC 184 / Building Smart

ISO TC 184 work deals with Industrial Automation technologies, including automated manufacturing equipment, control systems and the supporting information systems, communications and physical interfaces required to integrate them in the world of e-business. Major International companies from Automotive, Aeronautics, Space & Defence, Electric Device, Energy as well as main IT companies, research institutes, trade associations, consortia, and academia participate in the development of ISO TC 184 standards.

ISO TC 184 sub-committee 4 (SC4) Modelling of industrial, technical and scientific data to support electronic communication and commerce is dealing with standards for buildings. ISO 16739:2013 specifies a conceptual data schema and an exchange file format for Building Information Model (BIM) data. The conceptual schema is defined in EXPRESS data specification language. The standard exchange file format for exchanging and sharing data according to the conceptual schema is using the Clear text encoding of the exchange structure. Alternative exchange file formats can be used if they conform to the conceptual schema.

ISO 16739:2013 represents an open international standard for BIM data that is exchanged and shared among software applications used by the various participants in a building construction or facility management project.

ISO 16739:2013 consists of the data schema, represented as an EXPRESS schema specification, and reference data, represented as definitions of property and quantity names and descriptions.

A subset of the data schema and referenced data is referred to as a model view definition. A particular model view definition is defined to support one or many recognized workflows in the building construction and facility management industry sector. Each workflow identifies data exchange requirements for software applications. Conforming software applications need to identity the model view definition they conform to.

The following are within the scope of ISO 16739:2013: BIM exchange format definitions that are required during the life cycle phases of buildings: demonstrating the need; conception of need; outline feasibility; substantive feasibility study and outline financial authority; outline conceptual design; full conceptual design; coordinated design; procurement and full financial authority; production information; construction; operation and maintenance.

Building Smart is a national standardisation group organised by Standard Norway, see [54] and funded by Norwegian Directorate for Quality in Buildings.

5.10 European Telecommunications Standards Institute (ETSI)

ETSI is the 3rd of the three ESOs formally recognised by the EC as providing European Standards (ENs). It develops standards predominantly in the communications area but has recently moved ‘up the stack’ and is now developing standards and architectures for M2M and ITS. Members are collectively responsible for drafting and agreeing standards. VICINITY already includes member organisations among its partners.

5.10.1 TC Cyber

TC Cyber is addressing topics such as:

- 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

VICINITY should raise the topic of the need for a lightweight end-to-end encryption for the IoT in TC Cyber. The Chair of ETSI TC Cyber is a member of the VICINITY SAB and will help us to do this.

5.10.2 TC ITS

ETSI Intelligent Transport Systems (ITS) may be relevant to the Smart Grid and Parking pilot. However, ETSI ITS does not currently cover Smart Parking.

ETSI TC ITS does not yet see connected vehicles as members of the IoT and do not see the need for open communications except to support specific applications. Their progress, policies, plans and direction need to be monitored, but they are not yet ready to accommodate the open interfaces envisaged by VICINITY. VICINITY should look for opportunities to steer TC ITS towards a more open future in the IoT direction.

5.10.3 TC SmartM2M

ETSI TC SmartM2M was set up to develop specifications for M2M services and applications focussing on IoT and Smart Cities. It primarily supports European policy and regulatory requirements including mandates in the area of M2M and IoT. It identifies 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.

TC SmartM2M is currently mapping SAREF to the oneM2M Base Ontology and is also in the process of evolving SAREF and extending it to different domains. Therefore, it would be more useful for VICINITY to participate in SmartM2M rather than in oneM2M to ensure that SAREF meets the requirements of the architecture and pilots.

VICINITY partners UPM and CERTH are working on reference ontologies in ETSI TC SmartM2M.

5.11 oneM2M Partnership Project

The oneM2M Partnership Project involves 7 regional SDOs as 'Type 1' partners:

- Association of Radio Industries and Businesses (ARIB),
- Alliance for Telecommunications Industry Solutions (ATIS),
- China Communications Standards Association (CCSA),
- European Telecommunications Standards Institute (ETSI),
- Telecommunications Industry Association (TIA),
- Telecommunications Standards Development Society, India (TSDSI),
- Telecommunications Technology Association (TTA),
- Telecommunication Technology Committee (TTC).

This project therefore has a global reach and any member of one of these regional SDOs can participate in oneM2M.

The structure of oneM2M can be found in www.onem2m.org/about-onem2m/organisation-and-structure. The work on semantics / ontologies is carried out in WG MAS (Management Abstraction and Semantics). This is developing a Base Ontology based on the requirements of specific ontologies such as SAREF. Stages 1 and 2 have already been published as an ETSI TS. Stage 3 was finalised in August 2016 as part of oneM2M Release 2 [55].

5.12 Institute of Electrical and Electronics Engineers (IEEE)

The Standards Association of the Institute of Electrical and Electronics Engineers (IEEE-SA) is establishing a reference framework and architecture for IoT. The architectural framework defined in the IEEE 2413 standard aims to promote cross-domain interaction, aid system interoperability and functional compatibility across IOT systems. IEEE-SA also develops 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),
– Sensor Standards (IEEE 1451, IEEE 2700).

Standards relevant to VICINITY include IEEE 802 LAN/MAN Standards [56] and the Suggested Upper Merged Ontology (SUMO).

A particularly relevant body of the IEEE Internet of Things Initiative [57] This has published P2413 Architectural Framework for the Internet of Things (IoT).

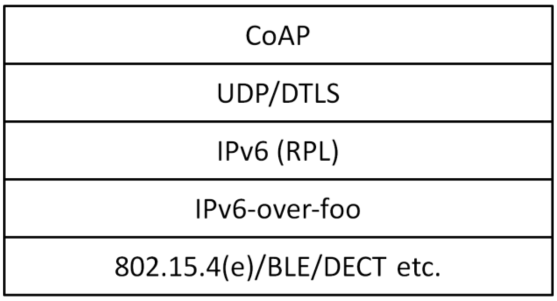
Participation in IEEE is via personal membership. Standards are agreed via ballot. A 75% 'yes' normally results in a standard being accepted for publication.

5.13 Internet Engineering Task Force (IETF)

The Internet Engineering Task Force (IETF) has developed the following standards relevant to VICINITY:

- Constrained Application Protocol (CoAP) which is a protocol for device communication over the Internet.
- 6LoWPAN for constrained radio links.
- ROLL which is a routing protocol for constrained-node networks.

Figure 21 shows a layered view of the IETF IoT protocol stack. Applications and devices are interconnected via IPv6 which has sufficient address space to be available on a wide variety of different devices and link layer technologies, each of which are tailored to meet the specifics demands of their domain: wired vs wireless, short vs long range, line of sight vs non LoS, high vs low data throughput, narrowband vs wide band, etc.



CoAP

UDP/DTLS

IPv6 (RPL)

IPv6-over-foo

802.15.4(e)/BLE/DECT etc.

Figure 21: IETF IoT protocol stacks.

The CoAP protocol specification was developed by the Constrained RESTful Environments (CoRE) WG and published as RFC 7252 in June 2014. CoAP uses the same RESTful principles as HTTP, but is much lighter so that it can be run on constrained devices. To achieve this, CoAP has a much lower header overhead and parsing complexity than HTTP. It uses a 4-bytes base binary header that may be followed by compact binary options and payload.

5.14 Integrating the Healthcare Enterprise (IHE)

IHE [58] is an initiative by healthcare professionals and industry to improve the way computer systems in healthcare share information. IHE promotes the coordinated use of established standards such as DICOM and HL7 to address specific clinical needs in support of optimal patient care. Systems developed in accordance with IHE communicate with one another better, are easier to implement, and enable care providers to use information more effectively. VICINITY will use IHE as follows:

- IHE Profiles will be used by the VICINITY eHealth at Home pilot..
- The IHE XDR has been selected by Continua for the exchange of clinical documents between healthcare enterprises and will also be used by the eHealth at Home pilot.

IHE specifications are considered to be mature as they stand and VICINITY will not need to modify them in order to use them effectively.

5.15 International Organisation for Standardisation (ISO)

ISO is a global level SDO and has worldwide representation from NSOs. Participation is normally only possible through accreditation by an NSO. The following are the TCs most relevant to VICINITY. The full list of ISO TCs is given in [59].

5.15.1 ISO TC 204 Intelligent Transport Systems

ISO TC 204 is closely integrated with CEN TC 278 as discussed in Section 5.6.4. WG16 covers ITS which is relevant to the Smart Grid and Parking pilot.

ISO/TS 21219 is a multi-part standards covering Traffic and travel information and Part 14 is under development which will cover Parking Information (TPEG2-PKI), Weather Information, Geographic Referencing, Traffic Flow and Prediction Appliances. VICINITY partner HITS is member of National Mirror Group of ISO TC 204/CEN TC 278 and should try to merge DATEX II and Exchange standards into one standard for ITS.

The work of the other WGs should be monitored to see how progress, policies, plans develop: they are not yet ready to accommodate the open interfaces envisaged by VICINITY. We should look for opportunities to influence a more open future in this WG.

5.15.2 ISO TC 215 Health Informatics

ISO TC 215 covers Health Informatics, which may be relevant to the VICINITY eHealth at Home pilot. Relevant work is the new ISO/NP TS 11633-1 Health Informatics, Info security management for remote maintenance of medical devices and MIS – Part 1 Requirements and risk analysis. VICINITY partner HITS is a member of National Mirror Group of ISO TC 215 and will monitor this.

5.16 ISO/IEC JTC1 Information Technology

JTC1/WG 10 is developing foundational standards for IoT to meet industrial requirements as well as user requirements. In 2017, WG 10 will deliver two standards of note. One is IoT Reference Architecture (IoT RA: ISO/IEC 30141) that defines reference models and architectural views, which can be easily extended to a real architecture. Second is definition and vocabulary for IoT (ISO/IEC 20924). Also, Technical Report on IoT Use-Cases will be continuously updated to collect various use cases including interoperability, smart manufacturing and smart wearable devices. Under the situation that support of interoperable IoT systems are getting more important, WG 10 will develop standards for Interoperability for IoT Systems (ISO/IEC 21823-1: Framework, ISO/IEC NP 21823-x(2): Semantic interoperability and ISO/IEC NP 21823-x(3): Network connectivity). WG 10 considers Wearable Technologies are one of key work scopes of WG 10 for fundamental IoT standardization, therefore standardization for Wearable Technologies is expected to be working items of WG

10 in 2017. For Systems Integration, WG 10 will keep cooperation with JTC 1 entities whose working items are related with IoT and Wearable Technologies as well as outside JTC 1.

VICINITY partner HITS is member of this WG. Currently, SRG6 is working on IoT use cases based on WG10_N0090 template, which currently includes:

- two IoT Use Cases from IEC SyCAA in area of Ambient Assistive Lliving (AAL)
- Smart Glasses use case from MPEG
- Smart Wearable Device use cases on "Searching for people with cognitive impairment" and "Sleep Monitoring System".
- Intelligent transport systems and Smart Parking (contributed by VICINITY), eHealth and ITS/Parking.

JTC1/WG7 has issued standards for Sensor Network Reference Architecture (SNRA) (ISO/IEC 29182) multipart standard; Part1: General overview and requirements; Part 2: Vocabulary and Terminology; Part 3: Reference Architecture Views; Part 4: Entity models; Part 5: Interface definitions; Part 6: Applications; Part 7: Interoperability guidelines. VICINITY partner HITS participates in WG 7.

ISO/IEC 20922:2016 is a Client Server publish/subscribe messaging transport protocol. It is light weight, open, simple, and designed so as to be easy to implement. These characteristics make it ideal for use in many situations, including constrained environments such as for communication in Machine to Machine (M2M) and Internet of Things (IoT) contexts where a small code footprint is required and/or network bandwidth is at a premium ISO/IEC 14543 covers Home and Building Electronic Systems (HBES).

ISO/IEC SC27 covers Development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as:

- Security requirements capture methodology;
- Management of information and ICT security; in particular information security management system (ISMS) standards, security processes, security controls and services;
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;
- Conformance assessment, accreditation and auditing requirements in the area of information security management systems;
- Security evaluation criteria and methodology.

SC 27 engages in active liaison and collaboration with appropriate bodies to ensure proper development and application of SC 27 standards and technical reports in relevant areas. ,

The following WGs may be relevant to the VICINITY architecture:

WG 1 – Information Security Management Systems, including SG-IoT meetings in October 2015, April 2016 and October 2016.

WG 2 – Cryptography and Security Mechanisms

WG 3 – Security Evaluation, testing and Specification

WG 4 – Security Controls and Services

WG 5 – Identity Management and Privacy Technologies

SC 27 proposes to take the following standards into account for a study period on "Guidelines for Privacy in Internet of Things (IoT): ISO/IEC 29100, 29101, 29134, 29151, 27018 and 30141.

VICINITY partner HITS is a member of SC 27/WG 1 and WG 5.

5.16.1 International Electric Committee (IEC)

In SAE terminology, 240 volt AC charging is known as Level 2 charging, and 500 volt DC high-current charging is known as DC Fast Charge. Owners can install a level 2 charging station at home, while businesses and local government provide level 2 and DC Fast Charge public charging stations that supply electricity for a fee or free.

The International Electrotechnical Commission *modes* definition (IEC 62196):

- *Mode 1* – slow charging from a regular electrical socket (single- or three-phase)
- *Mode 2* – slow charging from a regular socket but which equipped with some EV specific protection arrangement (e.g., the Park & Charge or the PARVE systems)
- *Mode 3* – slow or fast charging using a specific EV multi-pin socket with control and protection functions (e.g., SAE J1772 and IEC 62196)
- *Mode 4* – fast charging using some special charger technology such as CHAdeMO

There are three connection *cases*:

- *Case A* is any charger connected to the mains (the mains supply cable is usually attached to the charger) usually associated with modes 1 or 2.
- *Case B* is an on-board vehicle charger with a mains supply cable which can be detached from both the supply and the vehicle – usually mode 3.
- *Case C* is a dedicated charging station with DC supply to the vehicle. The mains supply cable may be permanently attached to the charge-station such as in mode 4.

There are four plug *types*:

- *Type 1* – single-phase vehicle coupler – reflecting the SAE J1772/2009 automotive plug specifications
- *Type 2* – single- and three-phase vehicle coupler – reflecting the VDE-AR-E 2623-2-2 plug specifications
- *Type 3* – single- and three-phase vehicle coupler equipped with safety shutters – reflecting the EV Plug Alliance proposal
- *Type 4* – fast charge coupler – for special systems such as CHAdeMO

Although the rechargeable electric vehicles and equipment can be recharged from a domestic wall socket, a charging station is usually accessible to multiple electric vehicles and has additional current or connection sensing mechanisms to disconnect the power when the EV is not charging.

There are two main types of safety sensor:

- Current sensors, which monitor the power consumed, and maintain the connection only if the demand is within a predetermined range. Sensor wires react more quickly, have fewer parts to fail and are possibly less expensive to design and implement. Current sensors however can use standard connectors and can readily provide an option for suppliers to monitor or charge for the electricity actually consumed.

- Additional physical 'sensor wires' which provide a feedback signal such as specified by the undermentioned SAE J1772 and IEC 62196 schemes that require special (multi-pin) power plug fittings.

Until 2013, there was an issue where Blink chargers were overheating and causing damage to both charger and car.[13][14] The solution employed by the company was to reduce the maximum current.[15]

5.16.2 ISO/IEC 20992 (MQTT)

MQTT is a Client Server publish/subscribe messaging transport protocol [60]. It is lightweight, open, simple and designed to be easy to implement. These characteristics make it ideal for use in many situations, including constrained environments such as for communication in IoT contexts where a small code footprint is required and/or network bandwidth is at a premium.

5.17 International Telecommunications Union (ITU)

5.17.1 SG16 Multimedia

ITU-T H.810 Series H: Audiovisual and Multimedia Systems – Interoperability design guidelines for personal health systems

5.17.2 SG20 IoT and its applications including smart cities and communities

This is relevant to IoT interoperability including APIs. SG20 has drafted an IoT Standards Roadmap [61]. It has been responsible for producing the Y-series of Recommendations for global information infrastructure, Internet protocol aspects and next-generation networks.

The ITU has a membership of approximately 700 organisations including the ministries of communication from most countries. SG20 has been defining key performance indicators for the performance of smart cities, which include metrics for the efficiency of services such as smart grids, e-health, e-transport and open data.

A new Work Item on a semantic ontology model for IoT is being proposed for worldwide acceptance based upon ETSI TR 101 584.

A new Work Item on “Requirements and capabilities for common IoT service discovery through IoT gateway in the IoT environments” has been proposed.

A new Work Item is proposed to study IPv6 potential and impact on the Internet of Things and smart cities and communities.

SG20 acts as a forum where the results of EU funded test-beds are shared on a worldwide basis. A recent example is crowd sourcing for multidisciplinary experiments gathering end-user interactions.

The services offered and the objectives of VICINITY trials could be contributed to SG20 with a view to developing new ITU Recommendations or Supplements. VICINITY could adopt ITU metrics for assessing its trials and contribute to the ongoing discussion of which metrics are most appropriate.

5.18 Open Interconnect Consortium (OIC)

The Open Interconnect Consortium (OIC) [62] published the first version of its IoTivity specification in September 2015. This is based around CoAP, the IETF protocol for device communication over Internet. They don't use ontologies but their data models are defined using RAML (a language for describing RESTful APIs), so VICINITY could not contribute much there. However, we can take those data models as input when defining requirements for the VICINITY ontology.

5.19 The Thread Group

Thread [63] was designed to create an effective way to connect and control products in the home. Thread was designed to have the following key features:

- Simple for consumers to use
- Always secure
- Power-efficient
- An open protocol that carries IPv6 natively
- Based on a robust mesh network with no single point of failure
- Runs over standard 802.15.4 radios
- Designed to support a wide variety of products for the home: appliances, access control, climate control, energy management, lighting, safety, and security

5.20 Universal Smart Energy Framework (USEF)

The USEF Foundation develops, maintains and audits the USED framework. USEF partners are working together to deliver the foundations of one integrated system which benefits all players - new and traditional energy companies and consumers.

The USEF Framework [43] is potentially relevant to VICINITY as a standards initiative on smart interconnected energy. VICINITY partner ENERCOUTIM should keep a watching brief and identify any implications for VICINITY.

5.21 World Wide Web Consortium (W3C)

The World Wide Web Consortium (W3C) is the main standards organization that develops standards for the Web. Two of its main activities are relevant to VICINITY: the Web of Data and the WoT.

From the Data activity (and its predecessor the Semantic Web one), VICINITY will use the set of standards defined for representing data on the Web (Resource Description Framework, RDF), describing ontologies that give meaning to such data (Web Ontology Language, OWL), querying such data (SPARQL Protocol and RDF Query Language), and providing REST interfaces to access them (Linked Data Platform, LDP).

From the current W3C WGs, the most relevant to VICINITY are:

- **W3C/OGC Spatial Data on the Web** (SDW) WG. The goal of the SDW WG is to clarify and formalize standards for the representation of spatio-temporal data, including data coming from sensors. This WG is explicitly chartered to work in collaboration with the Open Geospatial Consortium (OGC), in particular, the Spatial Data on the Web Task Force of the Geosemantics Domain WG. Among other deliverables, the SDW WG will standardize updated versions of the Time and the Semantic Sensor Network

(SSN) ontologies, previously defined in the scope of the W3C, and will provide best practices for publishing and using spatial data on the Web.

- **W3C Web of Things** (WoT) IG. Their goal is to identify requirements for the technology building blocks for the application layer that forms the WoT, with the idea of reaching out and collaborating with interested parties to create a new W3C WG. VICINITY should follow the discussions in the IG with a focus on the architectural components of the WoT needed to support WoT interoperability in the Web.
- **W3C Linked Building Data** (LBD) Community Group. The LBD CG aims to define existing and future use cases and requirements for linked data based applications across the life cycle of buildings. The group is following the same principles for publishing data on the Web as VICINITY will follow and has a focus on providing ontologies for representing Building Information Models following the IFC data model (an official ISO standard – ISO 16739:2013). Since building information is highly relevant for some of the VICINITY pilots, it is of interest to the project to follow the progress in this group.

VICINITY partner UPM is a member of these three WGs.

5.22 ZigBee Alliance

The ZigBee Alliance provides a foundation for the IoT and is well established in the AaI communications protocols area. In conjunction with the HomePlug Powerline Alliance it has developed Smart Energy Profile (SEP) 2.0 (e.g. for lightbulbs). ZigBee is not just about Transport and provides an example of creating Interoperability as a service.

VICINITY will use these profiles and develop the ZigBee example of Interoperability as a service into a device-independent semantic layer.

5.23 Analysis of VICINITY current engagement with Standards activity

	UNIKL	ATOS	CERTH	AAU	GRN	OTE	BVR	CAL	IS	UPM	GNOMON	TINYM	HITS	ENERC	MPH
AIOTI		🟩						🟩		🟩			🟩		
AllSeen Alliance					🟦										
BSI								🟩							
CECED					🟧										
CEN TC 204															
CEN TC 247															
CEN TC 251													🟩		
CEN TC 278								🟧					🟩		
CENELEC TC 205															
Continua											🟩		🟦		
Building Smart								🟧				🟩			
ETSI TC Cyber								🟧							
ETSI TC ITS								🟧							
ETSI TC SmartM2M			🟩							🟩					
oneM2M															
IEEE IoT WG	🟨														
IETF															
IHE															
ISO TC204								🟧					🟩		
ISO TC215													🟩		
ISO/IEC JTC1							🟦						🟩		
ITU-T SG16															
ITU-T SG20	🟦							🟨							
OIC															
Thread															
USEF														🟧	
W3C							🟦			🟩					
ZigBee Alliance															

Key:

🟩	Already involved and keen to continue
🟨	Recently involved – track record – keen to return
🟧	Recently involved – monitoring but not active contribution needed
🟦	Keen to become involved

Table 3: VICINITY partners engagement with standards activity

6 Conclusions & Recommendations

The current market place shows that IoT is a still growing area and many fora and consortia have been created to look at the various requirements for the IoT. These are very specific to their own area of expertise and in many cases are developing their own specifications and market requirements. For these reasons, it becomes more and more important to support interoperability between different levels of IoT systems in various IoT platforms based on different standards.

VICINITY does not have the resources to participate in all of the bodies relevant to IoT that are listed in Section 5. Based on the requirements of the VICINITY architecture, including the options for hardware, software and middleware platforms, the main priorities for standards involvement are listed below. A major focus will be on the standardisation of ontologies that are being defined in bodies such as oneM2M, ETSI SmartM2M and W3C, with the specific requirements of the VICINITY pilots being met in bodies such as Continua and ISO/IEC JTC1. Other bodies will be monitored for developments relevant to VICINITY:

Rec 1. A range of VICINITY partners should participate and contribute thought leadership to AIOTI, in particular WG3 (Standardisation and Privacy), but also in WG4 (Policy), WG5 (Smart Living Environment for Aging Well), WG7 (Wearables) for eHealth applications, WG8 (Smart Cities), WG9 (Smart Mobility) and WG13 (Smart Energy).

Rec 2. UPM and CERTH should participate in ETSI TC SmartM2M in order to ensure that the specific ontologies developed in ETSI (SAREF and its extensions) meet the requirements of the VICINITY pilots.

Rec 3. UPM should monitor developments in IoT ontologies and architectures in oneM2M to ensure they meet VICINITY requirements.

Rec 4. UPM to participate in the W3C/OGC Spatial Data on the Web WG to ensure that the SSN ontology meets the requirements of the VICINITY pilots.

Rec 5. VICINITY should participate in the W3C WoT IG (and in the future WG once it is chartered) to align the WoT framework defined there with that of VICINITY.

Rec 6. VICINITY should participate in the IEEE IoT WG, particularly to steer developments related to P2413 Architectural Framework for the IoT.

Rec 7. UNIKL and CAL should participate in ITU-T SG20 "IoT and its applications including smart cities and communities (SC&C)" to ensure that the sensor network and KPIs meet VICINITY requirements including low-energy and low-maintenance powering.

Rec 8. HITS should continue to participate in CEN TC 278 and ISO TC 204 to look for opportunities to steer these groups towards a more open IoT future in a direction beneficial to VICINITY objectives.

Rec 9. HITS should participate in ISO/IEC JTC1 participation in SC27 (Information security and privacy), WG7 (Sensor networks), WG10 (Internet of Things and SRG6: IoT Use cases). TC 1/WG 10 standards are expected to cope with the support of interoperable IoT systems.

Rec 10. CAL should participate in ETSI TC ITS, BSI EPL278 and other standards groups working on ITS should be monitored and policy setting meetings attended to encourage thinking about the inclusion of the kind of openness that is envisaged by VICINITY.

Rec 11. Existing representation from CAL in the ETSI Board and SSCC-CG should be used to monitor developments regarding the application of IoT to Smart Cities.

Rec 12. GNOMON should participate in the Continua Health Alliance to ensure that the approach and resulting specifications are aligned with VICINITY requirements.

Rec 13. ENERCOUTIM should keep a watching brief on the Universal Smart Energy Framework (USED) and identify any implications for VICINITY.

Rec 14. Gorenje should maintain membership of the European Committee of Domestic Equipment Manufacturers (CECED) and try to ensure that standards and specifications developed by them should align with VICINITY requirements.

Rec 15. TINYM should continue their involvement in Building Smart and related international standardisation initiatives in ISO in order to align the ISO 16739 standard with VICINITY requirements.

Annex A: Building domain standard considerations

From an information perspective, the building industry is highly complex. A building is usually a one-off design, and is so far difficult to produce using industrial approaches. Builders and property developers are mainly focusing on building as cheaply as possible, and usually give little attention to the operational phase and maintenance of the building.

This is reflected in the diversity of standards used in the building industry. These are often related to the materials and methods involved in the construction phase, and not to the operation of the building. Moreover, many professional disciplines are involved in the building process. Each of them have their specific standards, and the disciplines will often describe concepts differently in varying level of detail and focus. In addition, many of these standards are National and managed by local government regulatory authorities.

There are however also standards for some disciplines within the building that are relevant to the operational phase; also internationally. There are technical standards in electrical and technical installations in buildings. These are often associated with very specific functionality. In many cases, these standards have the transport layer and information model hardcoded together. Examples of this specific issue include wireless KNX, Wireless M-Bus, ModBus and CAN bus. The same challenge is found in some of the major standards for communication such as ZigBee.

Such generic standards ask for specific functionality for different domains and resulting in domain-specific versions of the standard. In the ZigBee standard we find Such domain-specific user profiles. This may result in varieties of the standard that often cannot talk neither the level of communication, nor the information level with other domain profiles in the same standard. An example is different implementations of ZigBee. The standard alliances tend to focus around technical and communicative interoperability, but only to a limited extent addresses semantic challenges.

This creates major challenges when the building industry tries to digitize the entire lifecycle of a building in an open information format. BuildingSMART [1] is a large standardization initiative that attempts to address this, both with regards to technical and semantic complexity in the global construction industry. The buildingSMART initiative is highly relevant to what we seek to achieve in the building domain in VICINITY.

BuildingSMART works with technical interoperability for data models used by different actors in building value chains. BuildingSMART also have an initiative for bridging semantic models. This is called buildingSMART Data Dictionary (bSDD) [1] and is a semantic dictionary which serves as an translation hub for all disciplines within the building domain. The BuildingSMART initiative is based on ISO 16739 [1] and is also denoted as IFC4.

The major application vendor digital tools for the construction industry supports IFC4 and can deliver and read Building Information Models (BIM) on an open BIM format. This means that they indirectly rely on bSDD.

Buildings are central objects in the Vicinity Smart Neighbourhood. When buildings are studied in neighbourhoods, and construction related information is lifted into other domains in a Smart City context (e.g. energy, ITS or home-based health care), the content and structure of bSDD will be a valuable contribution to the vision we have for Vicinity.

Annex B Smart Energy – Charging stations

An **electric vehicle charging station**, also called **EV charging station**, **electric recharging point**, **charging point**, **charge point** and **EVSE** (Electric Vehicle Supply Equipment), is an element in an infrastructure that supplies electric energy for the recharging of electric vehicles, such as plug-in electric vehicles, including electric cars, neighborhood electric vehicles and plug-in hybrids. https://en.wikipedia.org/wiki/Charging_station

Charging stations fall into four basic contexts:

1. Residential charging stations: An EV owner plugs in when he or she returns home, and the car recharges overnight. A home charging station usually has no user authentication, no metering, and may require wiring a dedicated circuit. Some portable chargers can also be wall mounted as charging stations.
2. Charging while parked (including public charging stations) – a commercial venture for a fee or free, offered in partnership with the owners of the parking lot. This charging may be slow or high speed and encourages EV owners to recharge their cars while they take advantage of nearby facilities. It can include parking stations, parking at malls, small centres, and train stations (or for a business's own employees).
3. Fast charging at public charging stations >40 kW, delivering over 60 miles (100 km) of range in 10–30 minutes. These chargers may be at rest stops to allow for longer distance trips. They may also be used regularly by commuters in metropolitan areas, and for charging while parked for shorter or longer periods. Common examples are CHAdeMO and SAE CCS chargers, and Tesla Superchargers.
4. Battery swaps or charges in under 15 minutes. A specified target for CARB credits for a zero-emission vehicle is adding 200 miles to its range in under 15 minutes. In 2014, this was not possible for charging electric vehicles, but it is achievable with EV battery swaps and Hydrogen Fuel Cell vehicles. It intends to match the refueling expectations of regular drivers.

Battery capacity and the capability of handling faster charging are both increasing, and methods of charging have needed to change and improve. New options have also been introduced (on a small scale, including mobile charging stations and charging via inductive charging mats). The differing needs and solutions of various manufacturers has slowed the emergence of standard charging methods, and in 2015, there is a strong recognition of the need for standardization.

7 References

1 www.vicinity-h2020.eu
2 ICT 30 – 2015: Internet of Things and Platforms for Connected Smart Objects - http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/914-ict-30-2015.html
3 EU Connected Digital Single Market https://www.eureporter.co/politics/2014/07/15/jean-claude-juncker-a-new-start-for-europe-my-agenda-for-jobs-growth-fairness-and-democratic-change/
4 http://www.lemaker.org/product-bananapro-specification.html
5 http://www.cubietruck.com/
6 https://www.kickstarter.com/projects/pine64/pine-a64-first-15-64-bit-single-board-super-comput/description
7 http://www.cnx-software.com/2016/03/01/raspberry-pi-3-odroid-c2-and-pine-a64-development-boards-comparison/
8 https://iotbytes.wordpress.com/popular-hardware-platforms-for-iot/
9 http://www.openhab.org/features/supported-technologies.html
10 https://github.com/openhab/openhab/wiki
11 http://devicehive.com
12 http://www.openremote.com
13 https://allseenalliance.org/framework
14 https://www.iotivity.org/
15 DAYARATHNA, M. Comparing 11 IoT Development Platforms. DZone - IoT Zone, Feb. 2016. Available online at https://dzone.com/articles/iot-software-platform-comparison
16 GAZIS, Vangelis, et al. A survey of technologies for the internet of things. In: 2015 International Wireless Communications and Mobile Computing Conference (IWCMC). IEEE, 2015. p. 1090-1095
17 PERERA, Srinath; SUHOTHAYAN, Sriskandarajah. Solution patterns for realtime streaming analytics. In: Proceedings of the 9th ACM International Conference on Distributed Event-Based Systems. ACM, 2015. p. 247-255
18 PERERA, Srinath. IoT Analytics: Using Big Data to Architect IoT Solutions. WSO2 White Paper. Nov. 2015. pp. 12
19 IoT-EPI Common Workshop, Valencia, Spain, 22-23.6.2016
20 Milan Zdravkovic, Miroslav Trajanovic, Joao Sarraipa, Ricardo Jardim-Goncalves, Mario Lezoche, et al. Survey of Internet-of-Things platforms. 6th International Conference on Information Society and Techology, ICIST 2016, Feb 2016, Kopaonik, Serbia. 1, pp.216-220. <hal-01298141>
21 PUIU, Dan, et al. CityPulse: Large Scale Data Analytics Framework for Smart Cities. IEEE Access, 2016, 4: 1086-1108
22 MINERAUD, Julien, et al. A gap analysis of Internet-of-Things platforms. Computer Communications, Volumes 89–90, 1 September 2016, p. 5–16.
23 How the AWS IoT platform works: https://aws.amazon.com/iot/how-it-works/
24 https://linksmart.eu/redmine/
25 SOLDATOS, John, et al. OpenIot: Open source internet-of-things in the cloud. In: Interoperability and Open-Source Solutions for the Internet of Things. Springer International Publishing, 2015. p. 13-25
26 FIWARE: www.fiware.org
27 "IoT LSP Standard Framework Concepts", Alliance for Internet of Things innovation WG3 (IoT Standardisation), Release 2.4, 2016.
28 Semantic Sensor Network Ontology, W3C First Public Working Draft 31 May 2016, https://www.w3.org/TR/vocab-ssn/
29 SensorML Specification, Version 1.0.1., http://www.ogcnetwork.net/SensorML_Spec
30 Media Types for Sensor Markup Language (SENML), https://tools.ietf.org/html/draft-jennings-senml-10

31 oneM2M Base Ontology, Latest Draft Specifications, http://www.onem2m.org/technical/latest-drafts
32 SAREF: the Smart Appliances REFerence ontology: https://w3id.org/saref
33 Martin, D. et al: OWL-S 1.2 Release. Available at http://www.ai.sri.com/daml/services/owl-s/1.2/, OWL-S (formerly DAMLS) Coalition, Dec. 2008
34 Farrell, J., Lausen, H.: Semantic Annotations for WSDL and XML Schema. W3C Recommendation. Available at http://www.w3.org/TR/sawsdl/, World Wide Web Consortium, Aug. 2007
35 de Bruijn, J. et al: Web Service Modeling Ontology (WSMO). W3C Member Submission. Available at http://www.w3.org/Submission/WSMO/, World Wide Web Consortium, June 2005.
36 de Bruijn, J. et al: The Web Service Modeling Language WSML: http://www.wsmo.org/wsml/wsml-syntax, ESSI WSML WG, 2008.
37 Web Service Modelling eXecution environment. Available at http://www.wsmx.org, DERI Galway and STI Innsbruck, 2008.
38 European Commission and TNO: "Smart Appliances REFerence ontology (SAREF)", April 2015.
39 S. Vinkovič, M. Ojsteršek, "The internet of things communication protocol for devices with low memory footprint," International journal of ad hoc and ubiquitous computing, 2014, pp. 1-11, http://www.inderscience.com/info/ingeneral/forthcoming.php?jcode=ijahuc
40 IETF RFC 2818 HTTP Over TLS http://tools.ietf.org/html/rfc2818 secure https communication
41 SmartGrids European Technology Platform: http://www.smartgrids.eu/ETPSmartGrids
42 "Internet of Things, IoT Semantic Interoperability: Research Challenges, Best Practices, Recommendations and Next Steps", IERC white paper: http://www.internet-of-things-research.eu/documents.htm
43 USEF Framework: http://usef.energy/Home.aspx
44 IHE Profiles: http://www.ihe.net/Profiles
45 Health Level 7 Standards: https://www.hl7.org
46 The DICOM Standard: http://dicom.nema.org/standard.html
47 Continua Health Alliance: http://www.continuaalliance.org
48 AllSeen Alliance - allseenalliance.org
49 BSI PAS 212 "Automatic resource discovery for the Internet of Things-Specification" - http://shop.bsigroup.com/ProductDetail/?pid=000000000030327418
50 European Committee of Domestic Equipment Manufacturers (CECED): http://www.ceced.eu/site-ceced.html
51 List of CEN technical Bodies: https://standards.cen.eu/dyn/www/f?p=CENWEB:6:::NO:::
52 Continua Alliance http://www.continuaalliance.org/about-the-alliance/join and www.iso.org/iso/catalogue_detail.htm?csnumber=69466
53 Personal Connected Health Alliance, White Paper on Fundamentals of Data Exchange, September 2015.
54 http://buildingsmart.org
55 http://www.onem2m.org/news-events/news/105-iot-to-further-expand-when-onem2m-releases-next-set-of-specs-this-autumn
56 IEEE 802 LAN/MAN Standards Committee - www.ieee802.org
57 IEEE IoT Initiative http://iot.ieee.org/about.html
58 Integrating the Healthcare Enterprise: http://www.ihe.net/
59 List of ISO Technical Committees: http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees.htm
60 http:// http://mqtt.org/
61 [JCA IoT and SC&C I-288 R1]
62 https://openconnectivity.org
63 The Thread Group - www.threadgroup.org