Project no.:	**610658**
Project full title:	**eWALL for Active Long Living**
Project Acronym:	**eWALL**
Deliverable no.:	**D7.5.2**
Title of the deliverable:	**Standardization contributions**

Contractual Date of Delivery to the CEC:	**31.10.2016**
Actual Date of Delivery to the CEC:	**31.10.2016**
Organisation name of lead contractor for this deliverable:	**Aalborg University**
Author(s):	**Albena Mihovska, Sofoklis Kyriazakos (AAU), Matthias Pocs (STELAR)**
Participants(s):	**P01, P13**
Work package contributing to the deliverable:	**WP7**
Nature:	**R**
Version:	**1.0**
Total number of pages:	**15**
Start date of project:	**01.11.2013**
Duration:	**36 months – 31.10.2016**

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 610658

Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Abstract:

This deliverable describes the standardization contributions of eWALL project during the 3rd project year.

Keyword list: standardization contribution, eWALL, ITU-T, Continua Alliance, ETSI, SMART BAN, CEN.

Document History

Version	Date	Author (Unit)	Description
0.1	Oct 5, 2016	Albena Mihovska	Started document
0.2	Oct 26, 2016	Matthias Pocs	Contributions
0.3	Oct 27, 2016	Albena Mihovska	Final draft
1.0	Oct 28, 2016	Sofoklis Kyriazakos	Final review and approval

Table of Contents

1 Executive Summary

Deliverable 7.5.2 reports on the eWALL standardisation activities during the final project year.

The FP7 project eWALL is an innovative and highly user-oriented research and development project that provides a smart ambient application platform for continuous support of clinically diagnosed patients experiencing chronic obstructive pulmonary deficiency (COPD) and mild cognitive impairments by monitoring and offering customised to the patient's needs services. The eWALL platform integrates sensors, actuators, reasoners, and the cloud to enable the patient-relevant personalisation.

A major role for making the project successful is to ensure that the eWALL technology is deployed and accepted by the end users is to make it compatible with standards that would guarantee the safety of the end users and the ease of deployment.

eWALL has put a great deal of effort on following the standardisation developments and contributing to standardisation with recommendations based on the project findings. At the same time, the project has been seeking to certify the eWALL devices with well-established certification bodies, such as Continua Alliance. Standardisation activities spanned to activities within ITU-T, ETSI, GISFI, and CEN TC 251. The main progress was registered through contributions to ETSI and CEN TC 251.

This deliverable describes the standardization activities of eWALL for the period 31.10.2015-31.10.2016, according to the standardization plan (D7.4). The document is organized as follows. Section 2 gives an introduction about the progress on standardization contributions. Section 3 focuses on the aspects of eWALL standardization within ITU-T and Continua. Section 4 focuses on the eWALL standardization within ETSI Smart BAN. Section 5 focuses on the eWALL standardization within CEN TC 251. It should be mentioned that here only the highlights of these activities have been reported, while full details are disclosed in D7.11. Section 6 concludes the deliverable.

2 Introduction

ICT research is a large field where a multitude of various specific scientific fields collaborate together in a thematic network to enable the realization of a complex application. Examples, of successful ICT applications, currently receiving a lot of research attention and, some of which have been even partially deployed, are smart grids, smart city, smart buildings, e-health, ambient assisted living (i.e., smart home), ICT-enabled manufacturing processes, self-driving cars, and a few others. A typical research team for such an application will include engineers from various fields, social scientists, medical scientists and social workers, designers, marketing experts, and on many occasions, the individual end users of the application, which get involved by means of pilot user trials. Such trend has been observed within the European –funded research programs that allow that the research is organized under a collaborative umbrella framework involving not only a team of inter-and multidisciplinary researchers and stakeholders but also, provide the means for highly international pan- European and inter-continental research. The European Commission has pointed out that such an approach has the potential to strengthen the scientific and technological base of the European industry and to encourage Europe's international competitiveness, while promoting research that supports EU policies.

The ICT area is a complex environment and participation to standardisation enables an efficient and needed way on reflecting on the various aspects and challenges arising from this complexity.

Internet of Things (IoT) is a prominent ICT paradigm, which enables information flows from/to and among highly distributed, heterogeneous, real and virtual devices (sensors, actuators, smart devices). IoT enables forms of collaboration and communication between people and things, and between things themselves, hitherto unknown and unimagined. The IoT can be defined simply as the Internet of connecting human and things. In the technical point of view, the IoT is defined as the Internet of connecting the human and things with identifiers and/or information processing capabilities. Comparing with the existing networks, the IoT has the following significant characteristics: connecting directly with the physical world without human intervention; autonomic networking of the IoT nodes; and autonomic interaction between the IoT nodes.

The IoT is a very complex network system, as it needs to connect a variety of different types of terminals and access networks for different application purposes.

The IoT concept is probably the best example of the innovations brought about by the IT and telecommunication convergence. Most IoT applications entail a large number of heterogeneous geographically distributed sensors. As a result, they need to handle many hundreds (sometimes thousands) of sensor streams. Many IoT elements and infrastructures (e.g., sensors, WSN, RFID), however, are location specific, resource-constrained and usually expensive to be developed and deployed. IoT is an essential enabler of the eWALL scenario and offered applications. The goal of eWALL by contributing to standardisation was to successfully bring to the relevant standardisation bodies requirements and technological issues that are of importance to defining the technical specifications for the related technologies and products.

The IoT operation relies on the automatic management, identification and use of a large number of heterogeneous physical and virtual objects (e.g., both physical and virtual representations), which are connected to the Internet. A common aspect of IoT applications is that many of them of practical interest involve control and monitoring functions, where human-in-the-loop actions are not required. As a matter of fact, a main reason for having many of these applications is to remove human intervention for improved efficiency, security, and safety.

Cloud computing and virtualization provide the means of immense distributed storage capacities that can solve the above problems. The cloud can provide the large-scale and long-lived storage and processing resources for the personalized ubiquitous applications delivered through the IoT networks as well as important backend resources. However, cloud-based platforms stay far from the real nodes connected to them. On the other hand, device-centric technologies and applications, such as IoT, constitute part of a local to the users and distributed in nature infrastructure, where a lot of personalized, and also, vital, data comes from sensors and actuators.

The main research challenge here is to integrate successfully the currently centralized concept of the cloud and its utilities to the highly distributed type of platforms on which IoT applications and services are based. An integrated combined framework utilizing the computing and storage capacity of the cloud to all ends of IoT communications and services can become a powerful tool to build new businesses.

M2M is a subset of the IoT, which creates a bridge between the real world (made of sensors, actuators, tags that are pervasive in our lives) and the virtual world (the Internet and its associated services).

IoT allows for the realization of many ICT scenarios (e.g., smart grid, self-driving cars, smart cities, e-Health) each having their own specific user and usage requirements. One common feature, however, is the involvement of a large number of devices in their realization. Some of those are mobile and relying on battery power for their operation. For example, even if the requirements for services delivered to e-Health or a smart home scenario may differ, common critical parameters will be security, mobility and reliability exist.

Typical IoT scenario characteristics are the unpredictability of the duration, location and time of communication between IoT objects as well as the need to enable the successful completion of the communication process and error-free conveying of the information.

Despite the huge research interest in IoT, a consensus on a common IoT architecture has not been reached yet within the research community. One possible reason for that is the lack of a joint technical and legal framework where the benefits of the various proposed concepts can be weighed against the interests of all stakeholders. Inter- and cross-disciplinary research can be an enabler for establishing this basis for building the future IoT ecosystem. Research and standardisation should continue to focus on fundamentally novel networking architecture concepts to support the collaborative behavior in an IoT system, including novel research on the required capabilities related to personalized service creation, identity-based user management, and IoT connectivity. Another key research aspect is to enable identification, naming, and addressing capabilities for supporting the connectivity in the end-user domain. Further, through the means of joint international inter- and cross-disciplinary research, an insight can be gained on how network and environmental awareness can be perceived, developed and expressed in an IoT scenario in order to lead to more flexible, efficient and modularized architectural paradigms.

2.1 E-Health and eWALL Technological Aspects of Relevance to Standardisation

ICT in general has the potential to solve significant social problems, such as the issues of aging, environmental problems, etc. Practically every application could benefit from using ICT in one or another enabling configuration.

An ICT-enabled e-Health service/application refers to systems, including computers, programs, databases, people, and operational support to manage the applications. Communication within an e-Health scenario refers to the information structures and networking that enable the communications between the services/applications and entities in the physical equipment. The physical equipment refers to the devices, sensors, and controllers that provide information to the ICT services/applications, and receive commands to effect the control of the devices in the physical equipment.

2.1.1 Cloud Computing for e-Health

More and more ICT services/applications rely on the cloud computing concept for the data management and processing. Whereas, cloud computing started with three main pillars, “Software as a Service-SaaS”; “Platform as a Service-PaaS”; and “Infrastructure as a Service-IaaS,” today, the number of functionalities, that are enabled as a service, is rapidly expanding. NaaS (Network as a Service), DaaS (Desktop as a Service), SDPaaS (Service Delivery Platform as a Service), TaaS (Things as a Service) [1]. The TaaS concept was the predecessor of the concept of fog computing, namely, TaaS allowed for some cloud characteristics, such as resource pooling, rapid elasticity and measured services to be implemented as a local content-centric cloud of gateways, providing services that map content information with thing resources, or make resources and data accessible by content regardless of physical location.

In an e-Health application scenario, we need to cater for the orchestration of available data collected from different enabled sensors, collecting data and intelligent decision support system output that will correlate available data sources, environment and ICT application context to propose the most accurate actions. To enable prompt and relevant decisions, semantic data correlations, are essential in order to provide an optimal situation reaction with the most optimal activity related visual data presentation [2]. The e-Health application requires a specific to its needs ontology that enables semantic sensor data correlation and semantic modelling of the middleware services that are distributed at the sensing and the cloud environments.

A common feature of an e-Health scenario, besides the enabled at all times communication and information access, is that most of the communicated and accessed, derives its value in real-time. For example, an e-Health scenario would provide a real-time feedback of the patient’s vital data.

The need to process the real-time data needs communication optimization algorithms where real and non-real time parameters information relevant to the particular scenario, can be included in the optimization functions. To this end, network solutions that allow for transparent communication over the full spectrum of available communication technologies and infrastructures (e.g., Ethernet, cable, fiber, Wi-Fi, ZigBee, 3G/4G/5G...) are needed, hereby taking into account (1) the quality of service (QoS) constraints (latency, reliability, bandwidth...) dictated by the ICT applications (collection of application-related parameters, collection of individual user demands..); (2) the availability of wireless/wireless technologies and their policies (e.g. cost, maximum allowed bandwidth usage); and (3) the dynamic properties of the different connection technologies (bandwidth, BER, transmission delay...). Different communication paths may be established depending on the nature of the traffic (e.g. real-time versus non real-time, critical versus non-critical, low versus high data rate) and the instantaneous properties of the different communication links.

The concept of ‘fog computing’ allows for offloading the cloud computing tasks to the edge of the network, closer to the application and is another enabler of real-time data processing [3], [4], [5]. For example, in an e-Health scenario [2], which enables remote care for the patient, the vital to the patient’s medical state information will come from the sensing environment installed at the patient’s home. A fog node, located closer to the sensing environment would implement real-time signal processing algorithms that would be responsible for all the real-time processing of the health-related collected data to enable a set of personalized services or that a medical staff intervenes timely in response to an alarm. An example of this scenario application is shown in Fig. 1

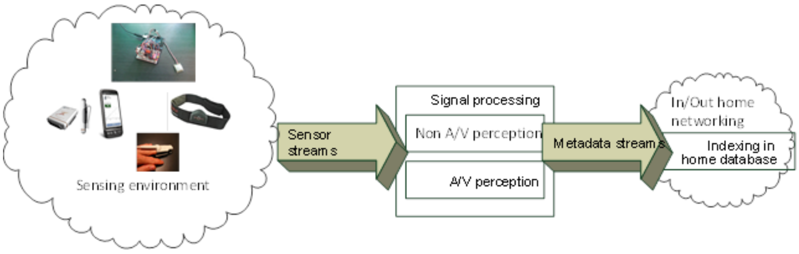

Fig.1 The concept of fog computing in an e-Health scenario.

2.1.2 Security and Privacy

ICT has the power to transform society and enable sustainability of the economy, on the other hand, the ICT services/applications raise new challenges. One important aspect that goes with ICT and digitalization is to cater for proper security solutions, especially because of the virtual and invisible to the end user in most cases handling of information, often of personal or critical nature.

The high number of the involved devices in an ICT scenario, most of which mobile, the various sources of collecting data (e.g., wireless sensors) and the unpredictability of the connections to be established, define a distributed type of topology. Security is becoming an increasingly important topic of concern, both due the more distributed nature of the communications, and for the most confidential or of critical to public safety nature of the data being collected and transferred.

Cybersecurity is one major area of research currently coming into focus both from an academic, industrial and also public point of view. It is crucial for the successful deployment of ICT applications to provide a sufficient level of security spanning from confidentiality of transmission to protection against attacks (e.g., denial of service-DoS and distributed denial of service (DDoS) where an intruder aims at disrupting the operation of the network (e.g., through jamming the communication or exhausting the energy of the key data processing devices). The larger the span of the emerging ICT applications, the larger the set of possible cybersecurity threats, and consequently, the larger the magnitude of their impact. In view of the cross-disciplinarity of the ICT applications and how they touch each aspect of the society existence, a breach in cybersecurity space, would have global consequences. Protection against cybersecurity crime will require that technical, legal, policy, social experts work jointly to build a solid ICT system. The challenge of cybersecurity, therefore, absolutely requires a multi-faceted international research approach and involvement of standardisation.

The focal point of an e-Health scenario is the human user. The analysis of the user’s needs and behaviors is essential for a human-centric operation, however, such an analysis is built on a lot of personal data that require to be stored somewhere. The acceptability of the e-Health system depends on the risks felt by the users, the public authorities and the policymakers. In certain e-Health scenarios (e.g., e-Health use cases), attackers may use the personal data for harmful purposes.

Security threats and attacks in an e-Health scenario can be classified as passive and active. For example a passive attack may occur after the sensitive personal data gets routed through the network. Attackers may change their destination or make routing inconsistent. User-centric data may get stolen by eavesdropping to the wireless communication media. An active attack may occur if the location of the user becomes known, which may lead to life threatening situations. The common design of sensor devices incorporates limited external security features and, therefore, makes them prone to physical tempering. This increases the vulnerability of the devices and poses more complex security challenges. The attacks to an e-Health personal network would most likely be due to eavesdropping and modification of the sensor data, allowing to trigger false alarms, denial of service, location and activity tracking of users, physical tampering with devices and jamming attacks [9].

The PbD was proposed for the eWALL system to enable the aspects of its products and services, whether standardized or specialized, for any personal identification or behavioral profiling purpose, offered by equipment providers, equipment integrators, system integrators and service providers. The approach should relieve caregivers and other users of any additional bureaucratic legal procedures that the technology deployment would imply. The PbD approach is very relevant for an e-Health scenario and should be explored further.

Such risks have legal, ethical and technical dimensions. One possible countermeasure is the proper user identification and putting in place intelligent Identity Management (IdM) mechanisms, which to involve all of the e-Health scenario elements [10]. The identification can be explained as an association of attributes, which represents identifiers. To make the communication within the HCS-N more efficient, one common device and object identifier would be beneficial [11-12]. [10] proposed a Computing Device Recognition (CDR) algorithm for automated and secure user and device identification to be applied in an HCS-N eHealth scenario. It allowed that the user could be identified and access various service delivered by heterogeneous devices. Another advantage is the ability for a user to define and manage his/her own rules in the stage of profile creation such as: device connectivity type (automatically or manually), services access permissions, number of computing devices as an input data for CDR procedure.

Privacy protecting technical concepts are key to the personal network of the eWALL user, where diverse user-centric decisions are based on the inputs received from the various sensing and monitoring devices comprising the user's ambient network. In addition, ethical requirements are also very relevant here, particularly for the scenarios involving secondary users (e.g., medical personnel, family caretakers). According to the EU and international law, people have the right to protection of their privacy and personal data. Personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Data protection law is made up of a broadly recognized set of principles: lawfulness, profiling prohibition, data availability, purpose limitation, data security, data subject rights, anonymity, responsibility and accountability. The right to privacy includes the right to control personal data. This means that the user must be aware of the data and the time period, for which their personal data are stored and who gets access to the information. Further, the user has the right to object to the data processing.

All these aspects have been the driver behind the chosen standardisation strategy of eWALL. The details about the chosen international standardisation working groups is given in the following sections.

It must be noted that the standardisation process is a time-consuming effort, and the reported activities have been ongoing during the eWALL lifetime. Therefore, some of these activities remain the same as reported in the previous eWALL Deliverable D7.5.1. However, we have decided to include these here for completeness as this is the final report on standardisation activities.

3 ITU-T and eWALL

ITU-T has been interested in standards for e-Health because ITU-T believes that e-Health systems can potentially transform healthcare through mobile health delivery, personalized medicine, and social media e-health applications. Reaching the potential for advancements in e-health will only be achieved through ICT standards efforts that facilitate interoperability among systems and devices, provide unqualified privacy and security, address the unique needs of the developing world, and leverage existing ubiquitous technologies such as social media applications and mobile devices. ITU-T published a Technology Report on E-health Standards and Interoperability in April 2012, which can be viewed here: https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000170001PDFE.pdf.

The following groups have been active within ITU-T on the topic of standards for e-Health:

3.1 ITU-T Study Group 16: e-health and standardization

Study Group 16 has been focused on defining recommendations for the interoperability among systems and on how to reduce the cost of devices through economies of scale, which are needed to enable a wide deployment of e-health applications (with an initial focus on telemedicine applications), in particular in developing countries. Consequently, the development of global international standards with the involvement of the major players (such as governments, inter-governmental organizations, non-governmental organizations, medical institutions and medical doctors) is a key factor to achieve these objectives.

In the Standardization Sector of the ITU (ITU-T), this is handled by Question 28/16 (Multimedia framework for e-health applications), which focuses on the standardization of multimedia systems to support e-health applications. Question 28 is allocated under ITU-T Study Group 16, which is the Lead Study Group on ubiquitous applications (“e-everything”, such as e-health and e-business). This high-level Question coordinates the technical standardization of multimedia systems and capabilities for e-health applications in ITU-T and will develop corresponding Recommendations.

Question 28/16 started its work on creating a roadmap of what standards exist, and it coordinates its planned actions with other organizations developing e-health standards via the e-Health Standardization Coordination Group (eHSCG) or specific liaisons with other bodies. It also provides support to the work in ITU-D SG 2.

The improvements and additions to the specific characteristics of multimedia systems and terminals is addressed within the relevant equipment related questions of Study Group 16.

A typical e-Health application architecture as considered by SG 16 is shown in Fig. 2.

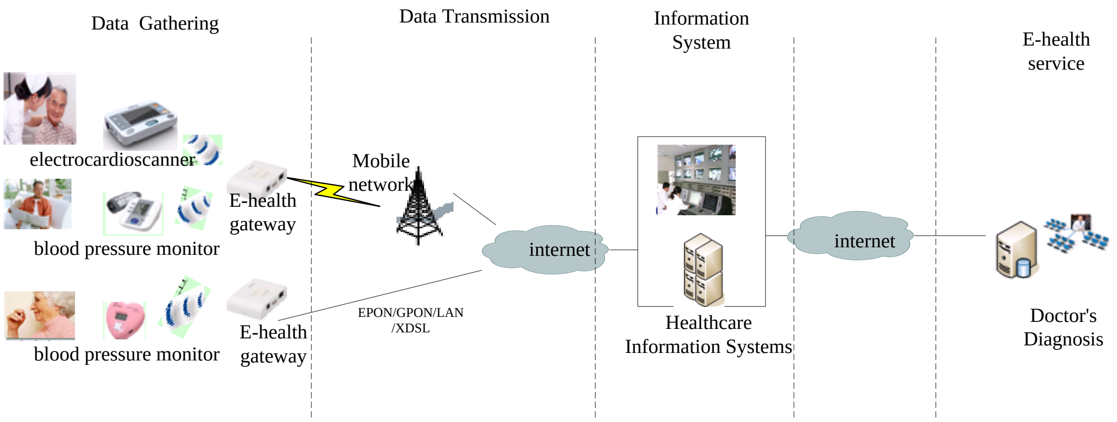

Fig.2 An e-Health application architecture as considered by ITU-T SG16

The E-health application architecture includes three parts: health data gathering, e-health platform and e-health service. The data gathering part include all kinds of e-health monitor devices and the e-health gateway, such as electro-cardio-scanner and blood pressure monitor. The e-Health monitor devices and the e-Health gateway form the wireless local area network (WLAN). The health consumer can use e-health monitor devices to gather the health data and transmit them to the e-health platform by the internet. The Healthcare Information Systems will be safe and manage all the gathering health data. At the same time, the Healthcare Information Systems open the user interface to the health consumer and the doctor. In the e-health service part, the doctor can log in the e-health platform, diagnose the user’s health data and form the health report to the health consumer.

3.2 eWALL and Continua Alliance

Continua Alliance and eWALL were discussed briefly in Section 3.1. At the moment, eWALL is performing the CHA compatibility implementation. eWALL has made the initial porting of the Continua Alliance antidote code to the WP3 needs. The C libraries are ported and embedded into the DGw C++ project, which is the first step in providing the Bluetooth and USB support for CA certified devices. Work is ongoing towards enabling end-to-end communication with the remaining components in the eWall system. The antidote structures need to be adapted to the eWall DGw structures, the CA callbacks should be forwarded to the DGw respective ones.

4 eWALL Standardization via Smart BAN ETSI

As it has been reported previously, eWALL was invited to join the SMART BAN ETSI Technical Committee in April 2015. The SmartBAN committee (TC SmartBAN) is developing standards for a dedicated BAN radio technology. This includes the following:

- The low complexity Medium Access Control (MAC) and routing requirements for SmartBANs
- An ultra-low power Physical Layer for on-body communications between a hub and sensor nodes interoperability over heterogeneous networks
- A system description, including an overview and use cases.

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

Currently, two standards are available for viewing.

- The TS 103 325 Smart Body Area Network (SmartBAN); Low Complexity Medium Access Control (MAC) for SmartBAN;
- TS 103 326 Smart Body Area Network (SmartBan); Enhanced Ultra-Low Power Physical Layer.

The eWALL activities within ETSI continued in the direction of exploring the open issue for radio channel modeling that reflects the effect of the human body and tissues on the RF signal propagation in order to enable efficient and reliable transmission of vital data within a smart body area network (S-BAN). Research reported in [6] showed that the impulse response of a signal traveling through the human body differentiates from the specifications of the IEEE 802.15.4a WPAN standard [13], which would mean that some S-BAN scenarios (e.g., implantable devices) will not be feasible when building on this technology. Therefore, the promising open research issues for enabling reliable S-BAN connectivity are towards RF interference mitigating technologies, energy-efficient short-range technologies, new channel models to account for the specifics of the human body medium and their effect on the S-BAN radio transmissions [6], [7] and a seamless handover between RF and VLC transmission technologies. Some initial proposals for integrating VLC into the AAL scenario were presented in [8].

5 eWALL Standardization via CEN TC 251

The following eWALL standardisation activities can be reported in relation to CEN TC 251. Please, note that the points given below are only the highlights of the activities and that full details can be found in D7.11.

- Consultation of eWALL partners by Stelar in the March 2016 meeting of the eWALL General Assembly in Rome, Italy [1], after having prepared partners by correspondence prior to the meeting;
- Election of eWALL representative as convenor of CEN TC 251 WG I, after discussion of nomination at two CEN TC 251 meetings in May and June 2016 and a formal two-month voting period among the 33 European standards bodies;
- At May 2016 meeting of CEN TC 251, presentation of eWALL representative on a proposal for a European privacy standard ("Standardisation request by European Commission for Data Protection by Design for development of eHealth products and services");
- Organisation of conference calls by eWALL representative with TC 251 privacy expert and TC 251 chairs and convenors;
- Participation in September 2016 conference call of TC 251 management team with eWALL representative in his capacity as WG I convenor, organised by Dutch national standards body NEN (TC 251 secretary);
- At November 2016 meeting of TC 251, discussion of eWALL proposal (forthcoming).

6 Conclusions

eWALL has been very active in all relevant standardisation activities. This has had a two-fold impact, on one side through contributions to standardisation, eWALL managed to inform and disseminate the project results, which will give it a permanent record by finding a place into the technical specifications, and will enable a final feasible from deployment point of view solution because the relevant aspects will be fed into the standardisation activities and considerations. On the other side, eWALL got a better understanding of some critical aspects that could be fed back into the project work in order to increase the project impact and enable exploitation of the project results.

Bibliography

[1] EU FP7 ICT project BeTaaS– Building the environment for the Things as a Service, http://www.betaas.eu/.

[2] EU FP7 ICT Project eWALL, url://ewallproject.eu

[3] CISCO: Visual Networking Index Global Mobile Data Traffic Forecast 2014–2019, CISCO whitepaper, (2015)

[4] I. Stojmenovic, “Fog computing: A cloud to the ground support for smart things and machine-to-machine networks,” *Telecommunication Networks and Applications Conference (ATNAC), 2014 Australasian*, pp. 117-122, November 2014.

[5] R. Craciunescu, A. Mihovska, M. Mihaylov, S. Kyriazakos, S. Halunga, R. Prasad, “Implementation of Fog Computing for Reliable E-Health Applications,” in *Proc. Of IEEE ASILOMAR Conf.*, November 2015, Pacific Grove, Ca. USA.

[6] P.V. Patel, M. Sarkar, et al., “Channel Modelling Based on Statistical Analysis for Brain-Computer-Interface (BCI) Applications,” in Proc. Of IEEE INFOCOM, April 2016, San Francisco, CA, USA.

[7] R. Prasad and A. Mihovska, New Horizons in Mobile and Wireless Communications: Volume 1 Radio Interfaces, Norwood MA: Artech House 2009.

[8] A. Kumar, A. Mihovska, S. Kyriazakos, and R. Prasad, “Visible Light Communications (VLC) for Ambient Assisted Living,” Springer International Journal on Wireless Personal Communications, October 2014, Vol. 78, Iss. 3, pp. 1699–1717.

[9] EU FP7 ICT project eWALL, D2.4, “Ethics, Privacy and Security,” April 2014, http://ewallproject.eu.

[10] V. Zdravkova, M. Mihaylov, A. Mihovska, and R. Prasad, “Single Thing Sign On Identity Management for Internet of Things,” in Proc. Of Wireless VITAE 2015, Hyderabad, India, December 2015.

[11] D. Todorov, Mechanics of User Identification and Authentication: Fundamentals of Identity Management. CRC Press, 2007.

[12] Z. Qin et al., “A Software Defined Networking Architecture for the Internet-of-Things,” in Proc. of IEEE NOMS, May 2014, Krakow, Poland.

[13] EU FP7 ICT project eWALL, D2.7, "Final user and system requirements and architecture," March 2015, http://ewallproject.eu.