Project no.: 610658

Project full title: eWALL for Active Long Living

Project Acronym: eWALL

Deliverable no.: D7.5.1

Title of the deliverable: Standardization contributions

Contractual Date of Delivery to the CEC:	**31.10.2015**
Actual Date of Delivery to the CEC:	**31.10.2015**
Organisation name of lead contractor for this deliverable:	**University of Zagreb**
	Author(s): **Albena Mihovska (AAU), Dina Simunic (UoZ), Michael Pocs (STELAR), Mihail Rumenov Mihaylov (AAU)**
Participants(s):	**P01, P12, , P13**
Work package contributing to the deliverable:	**WP7**
Nature:	**R**
Version:	**0.3**
Total number of pages:	**25**
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.

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

Document History

Version	Date	Author (Unit)	Description
0.1	Sept 29, 2015	D. Simunic (P12)	Started document
0.2	Sept 30, 2015	M.Pocs (P13)	CEN TC251
0.3	Oct 19, 2015	A.Mihovska (P1)	ITU-T, ETSI, Continua
1.0	Oct 27, 2015	A. Mihovska (P1)	Completed document

Table of Contents

1 Executive Summary

According to the World Health Organization, telemedicine is “the use of information and communication technology to deliver medical services and information from one location to another", while e-health is “a new term used to describe the combined use of electronic information and communication technology (ICT) in the health sector”.

Different from the single-purpose wireless system standards, the wireless technologies delivering eHealth services have the hard task of operating an ever-growing number of heterogeneous networked devices that can communicate with each other or with people or robots for satisfying very dynamic and high-level user expectations. One of the major problems identified in healthcare services is the lack of Information and Communication Technology (ICT) standards, especially for the interoperability related to the eHealth area.

The FP7 project eWALL is an innovative and highly user-oriented research and development project. 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.

This deliverable describes the standardization activities of eWALL for the period 31.10.2014-31.10.2015, 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. Section 6 concludes the deliverable.

…..

2 Introduction

eHealth is the application of Information and Communications Technologies (ICT) across the whole range of functions that affect the health sector. eHealth systems include tools for health authorities and professionals, from national to international, from the doctor to the hospital manager, nurses, data processing specialists, social security administrators and - of course - the patients, as well as personalized health systems for individuals and community. Examples include health information networks, electronic health records, telemedicine services, personal wearable and portable communicable systems including those for medical implants, health portals, and many other ICT-based tools assisting disease prevention, diagnosis, treatment, health monitoring and lifestyle management.

One of the major problems identified in healthcare services is the lack of ICT standards especially for interoperability related to the eHealth area. Traditional healthcare environments are extremely complex and challenging to manage, as they are required to cope with an assortment of individuals' and healthcare business conditions under various circumstances and with a number of resource constraints. According to the Office of the National Coordinator for Health Information Technology's annual report on EHR adoption [ONC2014], despite progress in establishing standards and services to support eHealth services, information exchange and interoperability, practice patterns have not changed to the point that healthcare providers share patient health information electronically across organizational, vendor, and geographical boundaries, or that patients are encouraged to be treated from home. In addition, electronic health information is not yet sufficiently standardized to allow seamless interoperability, as it is still inconsistently expressed through technical and medical vocabulary, structure, and format, thereby limiting the potential uses of the information to improve healthcare.

The lack of well-established standards limit the potential of eHealth solutions to bring in tremendous savings in patient treatment and hospitalisation as well as improving the quality of life (QoL) of the patients. In particular, chronically ill individuals can benefit largely from a better and more stimulating QoL.

eWALL targets two groups of chronically ill patients. One is the group with Chronic Obstructive Pulmonary Disease (COPD), and the other group are the sufferers of mild dementia. Elderly, are a sub-group that can largely benefit from eWALL, because in one or another way, this group requires more frequent medical support. The diseases targeted by eWALL take also a toll of the resilience of the family of the patient because these may increase the financial and legal vulnerability. In many countries, including those in economic transition, the members of the extended family, who may have been able to absorb the impact of caring across the family network in the past, now live far from their kin for economic reasons. This change is likely to result in an increase in the need for formal care in coming years.

2.1 Importance of eWALL for COPD Patients

COPD is a no communicable lung condition that, however, is a life-threatening disease that interferes with normal breathing – it is more than a "smoker's cough". More than 3 million people died of COPD in 2012, which is equal to 6% of all deaths globally that year. More than 90% of COPD deaths occur in low- and middle-income countries. The disease now affects men and women almost equally, due in part to increased tobacco use among women in high-income countries. COPD is not curable, but treatment can slow the progress of the disease.

COPD is characterized by a persistent blockage of airflow from the lungs. It is an under-diagnosed, life-threatening lung disease that interferes with normal breathing and is not fully reversible. The more familiar terms of chronic bronchitis and emphysema are no longer used; they are now included within the COPD diagnosis.

COPD is confirmed by a diagnostic test called "spirometry" that measures how much air a person can inhale and exhale, and how fast air can move into and out of the lungs. Because COPD develops slowly, it is frequently diagnosed in people aged 40 or older.

COPD is not curable. It is essential to stop smoking to prevent the progression of COPD. Various forms of treatment can help control its symptoms and increase QoL for people with the illness. For example, medicines that help dilate major air passages of the lungs can improve shortness of breath.

The availability of treatment options for COPD differ across varying resource settings. WHO has released a guideline (1) with specific recommendations for COPD management in primary health care in resource-constrained settings.

2.2 Importance of eWALL for Dementia Patients

Dementia is a syndrome – usually of a chronic or progressive nature – in which there is deterioration in cognitive function (i.e. the ability to process thought) beyond what might be expected from normal ageing. It affects memory, thinking, orientation, comprehension, calculation, learning capacity, language, and judgement. Consciousness is not affected. Alzheimer's disease is the most common form of dementia and possibly contributes to 60–70% of cases. Dementia affects each person in a different way, depending upon the impact of the disease and the person's pre-morbid personality. The problems linked to dementia can be understood in three stages:

- Early stage – first year or two;
- Middle stage – second to fourth or fifth years;
- Late stage – fifth year and after.

eWALL targets the group of patients in the early and possibly middle stage. In the early stage, a person may become forgetful, especially regarding things that just happened; may have some difficulty with communication, such as difficulty in finding words; may become lost in familiar places; may lose track of the time, including time of day, month, year, season; may have difficulty making decisions and carrying out complex household tasks. Mood and behaviour are also affected- the person may become less active and motivated and lose interest in activities and hobbies; may show mood changes, including depression or anxiety, and may react unusually angrily or aggressively on occasion. As the disease progresses, limitations become clearer and more restricting, and the above effects more severe.

2.3 Importance of eWALL for the Elderly and QoL

QoL is directly related to maintaining good mental health, which refers to a broad array of activities directly or indirectly related to the mental well-being component. This can be mapped to the definition of WHO on health: "A state of complete physical, mental and social well-being, and not merely the absence of disease." It is related to the promotion of well-being, the prevention of mental disorders, and the treatment and rehabilitation of people affected by mental disorders. Loneliness

and a change in lifestyle imposed by advanced age or chronic diseases, can severely disturb the mental health of the affected individuals leading to depression. Depression is different from usual mood fluctuations and short-lived emotional responses to challenges in everyday life. Especially, when long-lasting and with moderate or severe intensity, depression may become a serious health condition. Providing means and ambience where these individuals can feel like 'nothing has changed' or 'nothing is wrong' would have multi-fold impact, on the individuals, community, economy, society.

2.4 Summary

eWALL addresses both the substantial need for help from others that is required by people with chronic diseases and the significant impact on caregivers. eWALL is targeting a solution that can be built with commercially available devices as much as possible to make it attractive for end users. However, a number of new functionalities and technologies have been introduced to the eWALL platform and these require certification to make them deployment feasible. On the other hand, eWALL needs the support of standardisation to further spread the deployment capacity of the solution in order to achieve wide-scale societal and economic impact. Therefore, eWALL has been active to standardisation by bringing in knowledge on requirements, know-how and recommendations to help Working Groups on the related thematic areas to define their Technical Recommendations and Specifications documents. By participating, eWALL is bringing back to the consortium knowledge as well, helping to build a solid technological solution and product of a lasting impact.

3 ITU-T and eWALL

ITU-T has been interested in standards for e-Health because ITU-T believes that e-Hhealth 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. 1.

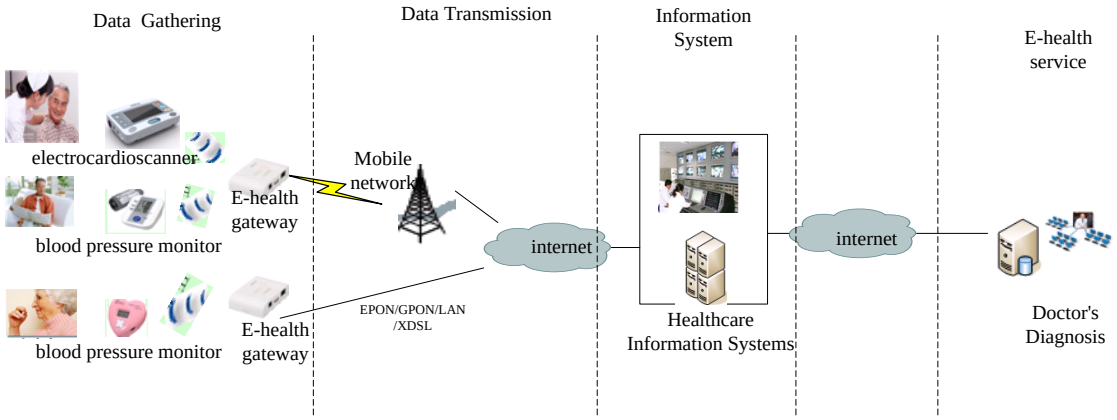

Figure 1 An e-Health application architecture as considered by ITU-T SG16

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.

eWALL has been very active within SG 16 Question 28. eWALL, represented by P01 attends SG16/28 meetings and has contributed to discussions in drafting the new edition of the guidelines (see bullet above). In June 2014, Q28/16 published a document HSTP-H810- 'Introduction to the ITU-T H.810 Continua Design Guidelines' available here: http://www.itu.int/pub/T-TUT-EHT-2014-H810, to provide a high level overview of the Continua Design Guidelines, an introduction to each of the standards and specifications that were chosen by its members to be part of the design guidelines, and the rationale behind their selection. eWALL was invited to demonstrate at the e-Health Interoperability event on February 10-12, 2015 in Geneva, Switzerland at the premises of ITU-T, with a special place at the showcasing event. Fig 2. and Fig. 3 show the photos from the

demonstration, jointly with Continua Alliance. The event included a testing component, where interoperability testing and conformance (Bluetooth Smart Agents and Health Record Network (HRN) Senders only) testing were conducted.

Figure 2 eWALL demonstration at the ITU-T and Continua Alliance interoperability event, 10-12/2, 2015

Figure 3 eWALL showcasing at the ITU-T and Continua Alliance interoperability event, 10-12/2, 2015

It is expected that either by the end of 2015 or the beginning of 2016 another such event will take place, to which eWALL has been invited.

3.2 ITU-T Study Group 17, Question 9: Telebiometrics

ITU-T Study Group 17 (SG17) coordinates security-related work across all ITU-T Study Groups. Often working in cooperation with other standards development organizations (SDOs) and various ICT industry consortia, SG17 deals with a broad range of standardization issues.

To give a few examples, SG17 is currently working on cyber security; security management; security architectures and frameworks; countering spam; identity management; the protection of personally identifiable information; and the security of applications and services for the Internet of Things (IoT), smart grid, smartphones, web services, social networks, cloud computing, mobile financial systems, IPTV and telebiometrics.

One key reference for security standards in use today is Recommendation ITU-T X.509 for electronic authentication over public networks. ITU-T X.509, a cornerstone in designing applications relating to public key infrastructure (PKI), is used in a wide range of applications; from securing the connection between a browser and a server on the web, to providing digital signatures that enable e-commerce transactions to be conducted with the same confidence as in a traditional system. Without wide acceptance of the standard, the rise of e-business would have been impossible.

SG17 is coordinating standardization work covering cyber security, e-health, open identity trust framework, Near Field Communication (NFC) security, and Child Online Protection.

Security is an essential feature for ensuring feasibility of the eWALL solution. eWALL joined the SG17 activities during the meeting in September 2015. In particular Q10/17 deals with Identity Management Architecture and Mechanisms. Some research work in this regard has been done by P01, on *Single-Thing Sign-On Identity Management for IoT*.

Identity management (IdM) is the management of the life cycle and use (creation, maintenance, utilization, provisioning, and revocation) of credentials, identifiers, attributes, authentication, attestation, and patterns by which entities (e.g., service providers, end-user, social networks, organizations, network devices, applications and services) are known with some level of trust. Depending on the context, multiple identities may exist for a single entity at differing security requirements, and at multiple locations. In the cloud and public networks, IdM discusses trusted information exchange between authorized entities that is based on validation and assertion of identities across distributed systems. IdM enables the protection of information and ensures that only authorized information is disseminated. IdM is a key component to the proper operations of telecommunication/ICT networks, (e.g., Internet of Things (IoT), cloud and mobile computing, services, and products) because it supports establishing and maintaining trusted communications. It not only supports authentication of an entity's identity, it also permits authorization of privileges, easy change of privileges when an entity's role changes, delegation, nomadicity, and other significant identity-based services.

IdM is a critical component in managing network security and enabling the nomadic, on-demand access to networks and e-services that end-users' expect today. Along with other defensive mechanisms, IdM helps to prevent fraud and identity theft and thereby increases users' confidence that e-transactions are secure and reliable (e.g., IoT, and cloud and mobile computing systems that are not directly controlled by the user organization).

IoT represents a unique interconnected system, which enables devices to communicate globally using set of standard protocols and connecting various heterogeneous networks. By means of a unique identifier (ID) IoT objects are able to communicate directly with each other [1]. In the context of IoT, the concept of identity extends to things. Identities can be considered as end points so that it is easy to ensure access to that thing endpoint independently.

The user identification process can be explained as an interaction whereby the user identity is provided to the security system. The identification provides access to and the modification of data by a certain personal, and enables services and communications to be customized [3]. In IoT context, identification can be explained as an association of attributes which represents identifiers.

To make the communication within IoT more efficient, one common device and object identifier would be beneficial [2] [3].

Various methods for user identification and attractive Identity Management (IdM) mechanisms, such as Single Sign On (SSO) have been proposed [2] [4], whereby the user effort of remembering passwords is simplified on a web level. L. Some early solutions to IoT IdM [5] are now being implemented but they still need improvement and standardization [4], [6]. TIdM for M2M is represented by authentication of multiple user's devices where the user can access a particular single service with all of his/her devices after performing initial authentication only on one device. The scenario adopted here assumes that the user will be able to access multiple services on a number of different devices by authenticating only to one of those devices. The access to connected shared devices will enable gathering contextual metadata and sensors data and will enable user centered responsive services. The enabling IdM feature is introduced by as Single Thing Sign On (STSO), which among others addresses challenges, such as heterogeneous networks with minimum human interaction, how to enable successful communication among personalized devices, and privacy.

To address the identity issues related to the proposed STSO IdM in IoT Computing Device Recognition (CDR) algorithm for automated and secured user and device identification was proposed [REF to paper GWS]. The proposed idea is to enable IdM for the identification of the user across multiple domains. The STSO IdM is based on the federated IdM system model proposed in [2]. The high-level system architecture is shown in Fig.4.

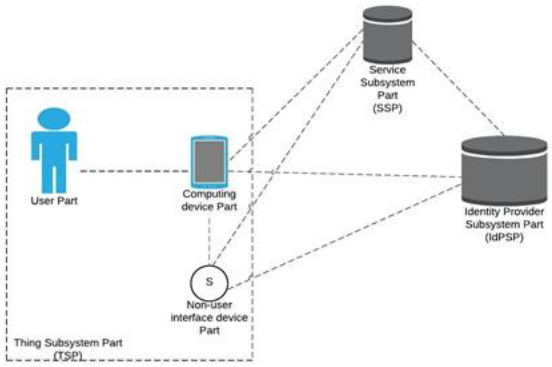

Figure 4 High - level IdM system structure.

The main physical entities of the system in Fig. 4 are the following:

- Thing Subsystem Part (TSP) - it represents the "things" in IoT such as users, smart computing devices, sensors and actuators. All of these take an important role in the user identity process by providing identities to the Identity Provider Subsystem Part (IdPSP). TSP is divided into three separate subsystems as follows:
    - User as a Part (UP) - in the proposed IdM system, the user is an actor, being a part of the system, who access multiple services by using his/her device(s). User identity data is obtained and provided by IdPSP.
    - Computing Device Part (CDP) - it is a functional layer residing in a user device and serve for providing middleware functionalities for the system. From security point of view, this part is needed to prevent unauthorized data modification and corruption.

- Non-user interface Device Part (Non-userIntDP) - this part is responsible for collecting accurate information from personal and/or shared non-user interface devices regarding users' needs. In that way, it supports SSP to provide always on time responsive services to the users.

- Identity Provider Subsystem Part (IdPSP) - the responsibility of the IdPSP is to store all the identity data. In addition, it is also responsible for the user, device and service authentication. Also, access to the non-user interface devices is managed by IdPSP. It can be remotely or locally located and one of the main benefits is that the IdPSP can provide communication and different functionalities automatically.
- Service Subsystem Part (SSP) - is a part of the proposed IdM service layer that enables authentication of a user or "things" both for local or remote services.

The design of the proposed IdM system allows multiple IdPSs management by multiple IdPs. The IdPSPs provides identity storage information, features for searching and discovering from a device perspective in an easier way and thus the latter is able to establish dynamic connections. The regular user can create a private subsystem of identifiers for his devices and established identities, which can be further provided to an IdPSP to manage them.

The general STSO connection procedure is shown in Fig. 5

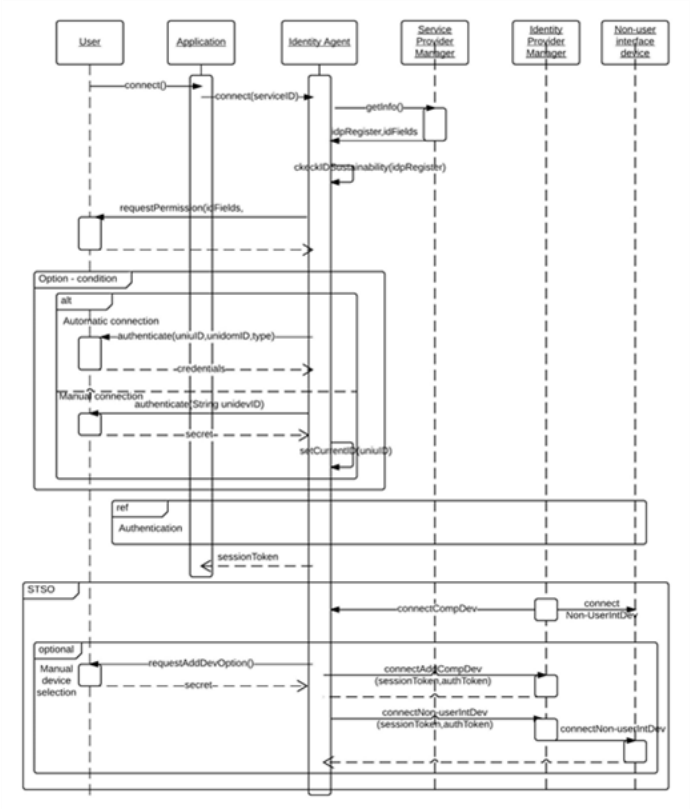

Figure 5 STSO connection sequence diagram.

Let us consider a case where a given computing device is utilized by a human user and the latter intends to connect locally or remotely to an available service through a certain application. The user may use beforehand applications, which require an automatic connection to the service, independently of the user's intentions. The sequence flow is as follows:

1) Application sends connect request to IdentityAgent providing service ID or alternative information related to requested service.

2) IdentityAgent uses the provided service information in order to establish communication with related ServiceManager and learn about IdPs relationships with the service and the required identity fields.

3) IdentityAgent obtains certain information associated to desired service from ServiceProviderManager.

4) IdentityAgent checks whether the provided computing device identity is active (if there is any) and appropriate for the service by using IdP list related to the service.

5) Subsequently, IdentityAgent notifies the user about the required identity data fields and gives an option for identity switch based on service requirements.

There are two possible alternative login mechanisms as shown in Fig. 5 The first one is an optional automated connection where all of the devices related to the user are automatically connected based on only one thing identification. If certain computing device(s) is (are) recognized by IdPs regarding user's preferences, STSO is activated.

The second is a manual connection procedure, whereby the user may manually confirm the identity and choose a device. Then, the provided thing's credentials should be checked by the IdentityAgent or IdP, which are required parties in the authentication procedure

Once the authentication is successfully completed, sessionToken is being set from IdentityProviderManager and send to the IdentityAgent. The latter sends a received sessionToken to the Application, which needs that token in order to establish its own communication to the service without elaborating with IdentityAgent.

The connection procedure includes an STSO feature where the IdentityProviderManager sends the connection device a request to, both, the computing and non-user interface devices groups related to the current user profile. That allows the automatic connection to the other user-related devices, after one of the things (user or computing device) is identified and connected. The procedure is enabled by a recorded connection in the ConnMsg class managed by the IdentityManagerProvider.

As an optional step, the user can choose manually devices, which he/she would like to utilize. In this case, either the IdentityAgent would ask whether they would like to access the service by means of the personal devices, or the user might agree and choose some additional devices and specify a secret key derived as an authToken. The latter will be used in the message send to the IdentityProviderManager afterwards.

When the ServiceManagerProvider requests authentication from the IdentityProviderManager, then:

1) The IdentityAgent sends a message to the IdentityProviderManager to request a connection to the additional computing devices and non-user interface devices as per the user's preferences. The message contains the authToken and sessionToken.

2) The IdentityManagerProvider receives the message for connecting to the additional devices, performs the authentication and sends a connection message to the targeted devices, if the authentication is successful.

In order to support STSO IdM, we propose a Computing Device Recognition (CDR) algorithm for user identification. The CDR algorithm does not exclude the most commonly adopted method for identification - username and password. It can be considered as an additional feature that simplifies

the authentication (automatic and less user intervention) but manual authentication can still optionally be used. The CDR algorithm is shown in Fig.6.

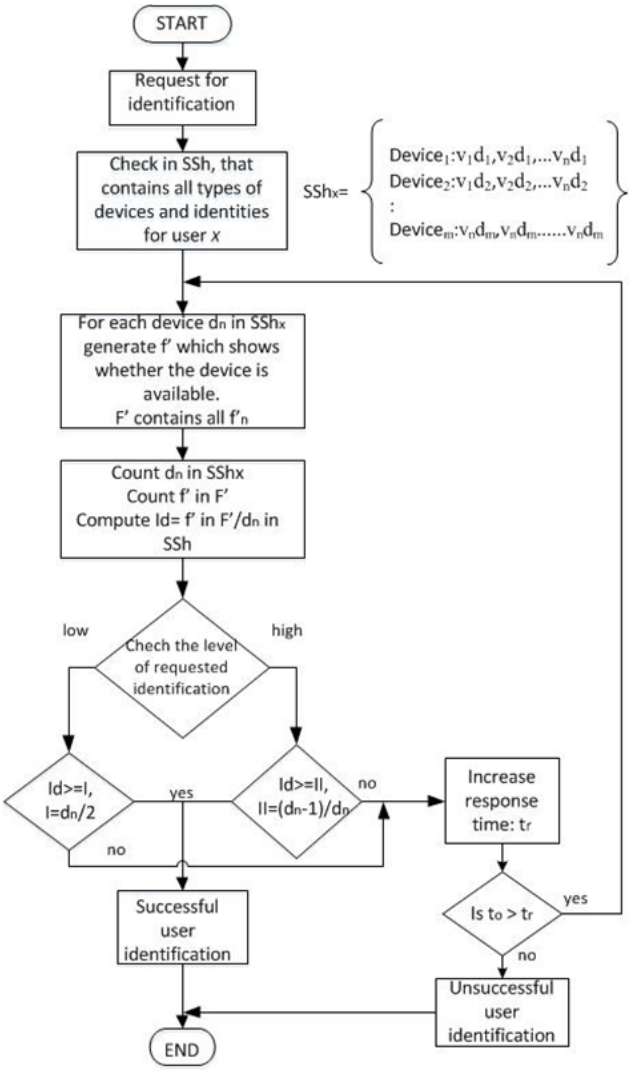

Figure 6 CDR identification algorithm.

The user's types of device identities ($v_n d_m$) are stored in a Smart Sheet (*SSh*). SSh_x is unique list of devices pointing to user *x*. Each device *d* is recorded to the SSh_x list with a reference number within the interval *[1-m]*. For each device in the *SSh* list, there is a set of different types of identifiers *v*, with a reference number within the interval *[1-n]*, which is assigned to the particular device d_m. If a request for identification from one of the listed and registered devices in a certain domain is received, the register automatically starts to search if there are other user devices and how many of them are available in the local domain. The user is able to define the level of security by manipulating the number of the devices needed for a proof of user identity. For example a certain user may create a policy for 3 out of 5 personal devices simultaneous recognition for automatic user

identity recognition. The user is a part of the Internet of people whereby he/she plays the role of manager of the rules in the system, regarding his/her preferences and wishes.

The available user's computing devices are counted and written in *F'sheet*. After that, the algorithm computes the *Id* index which shows the ratio between the entire devices stored in the SSh and those which are available in the *F' sheet* at a certain moment. Then, the level of required identification is checked. Here, two scenarios are available – for high and low level of identification depending on the user's or services' rules. If the level is low, the algorithm compares whether *Id* is bigger or equal to *I*. In that case, the ratio *I* is equal to at least half of the declared devices in *SSh* which must be discovered and recognized.

If that expectation is true, the identification of the user is successful. If not, the response time t_r is increased and compared with the timeout t_o for the service so the the process is started again until $t_o > t_r$. If the level is high – that the *Id* should be compared to *II index* which allows only one of the user computing device to be unavailable. If that expectation is true, the identification of the user is successful. If not, the process is started again until the timeout t_o for the service expires. A coefficient which defines the identification rate of the computing device is proposed in order to be used for the identification assessment within the CDR algorithm,

$$\mathrm{Ir_{cd}} = \frac{N_{cd}}{M_{cd}}$$

where $\mathrm{Ir_{cd}}$ is an identification rate coefficient of the computing device N_{cd} is a number of identified computing devices *(cd)* related to the particular user M_{cd} is a total number of predefined computing devices *(cd*) required for the identification . Ircd is equal to the number of identified computing devices related to the particular user over the total required number of predefined computing devices necessary for the identification procedure.

The eWALL system is composed of two main subsystems: the eWALL Sensing Environment and the eWALL Cloud. The eWALL Sensing Environment - is deployed over a physical space and interacts with the primary user. A Home Sensing Environment, operates in the domestic surroundings of the user. It monitors the status of environmental parameter such as humidity, temperature, luminosity, motion etc. A Mobile Sensing Environment would operate around the user and collect data from wearable devices. The data would be transferred to the home device gateway wirelessly when the user is within the communication range of it. Such wearables could be smartphones, pulse and blood oxygen saturation sensors, body temperature sensors, etc.

The eWALL Cloud would handle the data processing and storage whereby the eWALL Cloud is connected to the home environment of each user. Based on actions performed within the Cloud environment, personalized services and applications will be offered to the corresponding user.

The implementation of STSO IdM is proposed as subsystems components to be included in the eWALL architecture shown in Fig. 6 with the benefits of improved eWALL user identification, better mobility and more responsive eWALL applications.

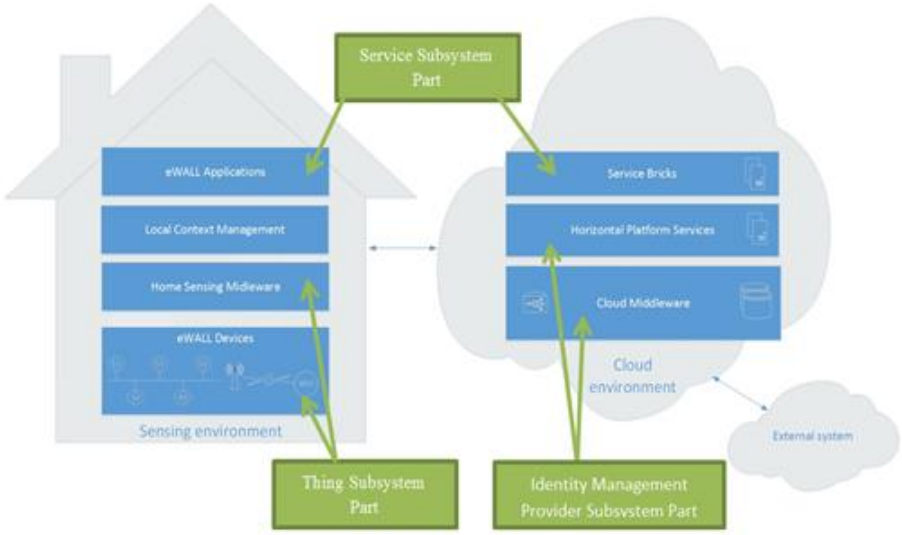

Figure 7 Implementation of STSO IdM subsystem parts in eWALL

TSP resides on the eWALL devices and Home Sensing Middleware components of eWALL where the eWALL users, sensors and computing devices could be assumed as part of the infrastructure, when referring to IoT and IdM. The Identity Agent should be installed on the eWALL primary user's computing devices, in order to enable the STSO feature.

IdPSP should be deployed as part of the Cloud Middleware and as a part of the Horizontal Platform Services where the user profile information is stored and managed at a cloud level. The IdentityManagerProvider should be implemented on a cloud middleware level to enable identity functionalities such as thing identity creation, management and deletion. What is missing for the eWALL system on a cloud level is a device identity management related to a certain user.

SSP is already represented in eWALL by User profiling functionalities the respective applications and services assignment to a certain user.

It is proposed to include the implementation of the STSO IdM within eWALL as a part of the holistic architecture of the platform, rather than as a single component or plug in. This would affect the overall architecture and would require dedicated C++ components to be implemented on a DeviceGateway level while other Java software artefacts should be deployed on a cloud level. The implementation may also cause changes in the JSON data format used for the sensors and actuators data representation and exchange, as well as it will require storing of additional device identity data both on the homePC (CouchDB) and eWALL cloud (MongoDB) databases. By introducing and implementing the IdentityAgent and IdentityProvider, eWALL will be able to extend further with adoption of the CDR algorithm where the user input efforts will be minimized. The password retyping and remembering will be substituted by the algorithm, which will contribute for simplifying the system and improving the privacy and security.

A number of advantages should be summarized as follows:

- CDR algorithm will improve the eWALL system in terms of usability and ease of use. It also is a way of performing better user experience, improved personalization and minimizing the need of user input which is important from senior or cognitive impaired users' point of view.

- STSO IdM will improve the eWALL system in terms of mobility and inner system sites roaming – by ensuring user identification and eWALL application access.
- STSO will add value to the eWALL system by providing Service orientation and ensuring always responsive services
- Personalization and privacy of services by improved ability for the user to create the rules for identification within the eWALL system.
- STSO IdM and CDR algorithm will improve the security by reducing the possibility for personal data abuse or unwanted system intrusion.

With introducing the STSO IdM in eWALL both the users and the business parties will benefit from better utilized sensing infrastructure, seamless roaming between eWALL sensing environments, improved personalization and security of the services and better monitoring of the patients.

Another advantage is that based on only one profile for STSO IdM, the user could be identified and be able to utilize various services by using myriad of devices. Furthermore, the user will be able 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.

The next meeting of SG17 is scheduled for March 14-23, 2015 and eWALL will continue to contribute to Q10/17, Q7/17.

3.3 ITU-T Focus Group on Machine-to-Machine Service Layer

This Focus group terminated its activities in 2013 but it is included here because it gave some useful insights for steering the ITU-T work towards the importance of machine-to-machine (M2M) applications as a key enabler for various business areas, including e-Health, and gave rise to considering this area within the framework of within other ITU-T Study groups. A common M2M service layer, agreed at the global level involving stakeholders from the M2M and vertical market communities, was considered to provide for a cost-efficient platform, which can be easily deployed in hardware and software, in a multi-vendor environment, and across sectors. The Focus Group on the M2M service layer (FG M2M) studied activities undertaken by various standards developing organizations in the field of M2M service layer specifications to identify key requirements for a common M2M service layer.
FG M2M identified a minimum set of common requirements of vertical markets, focusing initially on the health-care market and application programming interfaces (APIs) and protocols supporting e-health applications and services, and drafted technical reports in these areas. The various outputs of this work can be found here: http://www.itu.int/en/ITU-T/focusgroups/m2m/Pages/default.aspx.

Because eWALL started activities after the FG had been terminated, eWALL did not participate to this FG.

3.4 ITU-D: ICT Applications for e-health

e-Health is an integrated system of healthcare delivery that employs telecommunications/ICTs as a substitute for face to-face contact between medical staff and patient. It includes many applications, such as telemedicine, electronic medical records, medical consultation at a distance, medical consultation between rural medical centres and urban hospitals, etc. e-Health provides for transmission, storage and retrieval of medical information in digital form between doctors, nurses, other medical staff and patients for clinical, educational and administrative purposes, both at the local site (your workplace) and at a distance (remote workplaces). In some developing countries1, the number of mobile phones has overtaken the number of fixed phones, and the mobile telecommunication network could be considered a more attractive platform for the introduction of e health services.

e-Health is playing a very important role in healthcare delivery in developing countries, where the acute shortage of doctors, nurses and paramedics is directly proportional to the enormous unsatisfied demand for health services. Some developing countries have already successfully implemented small pilot telemedicine projects, and they are looking forward to proceeding further by considering the development of e health master plans, as recommended by the World Health Organization in its Resolution WHA58.28 in May 2005, which aims, in particular, at reducing disparities with regard to medical services between urban and rural areas and pays special attention to the least developed countries (LDCs).

Within ITU-D, Question 2/2 deals with ICTs for e-health. In particular, the Question studies:

- How to take further steps to assist in raising the awareness of decision-makers, regulators, telecommunication operators, donors and customers about the role of ICTs in improving healthcare delivery in developing countries.
- How to encourage collaboration and commitment between the telecommunication sector and the health sector in developing countries, in order to maximize the utilization of limited resources on both sides for implementing e health services.
- How to continue to disseminate experiences and best practices with the use of ICTs in e-Health in developing countries.
- How to encourage cooperation among developing and developed countries in the field of mobile e health solutions and services.
- How to promote the development of technical standards for e health applications in conjunction with ITU-T. In particular, develop guidelines for developing countries on how to use such standards.
- How to introduce and disseminate ITU technical standards related to e health for developing countries.

  The outputs from this Question will include:

  a) Guidelines on how to draft the telecommunication/ICT part of an e-Health master plan.

  b) Guidelines with regard to the use of mobile telecommunications for e-Health solutions in developing countries.

  c) Collection and summary of the requirements and effectiveness of telecommunication infrastructure for the successful implementation of e health applications, taking into account the environment of developing countries.

d) Dissemination of the technical standard related to the introduction of e health services in developing countries.

e) Collaboration with ITU-T Study Group 16 in order to accelerate the elaboration of technical standards for e health applications.

f) Collaboration with the relevant BDT programme, if so requested, to support implementation of the telecommunication/ICT component of e-Health projects in developing countries, including advice on best practices on how to train developing countries in the use of the telecommunication/ICT component of e health projects.

g) Sharing and dissemination of best practices on e-health applications in developing countries using the ITU/BDT website, in close collaboration with the relevant BDT programme.

This Question aims at stimulating collaboration between the telecommunication/ICT and health communities, between developed and developing countries, and among developing countries. The experience gained from telecommunications/ICT for e-Health applications in developing countries will also be expected to benefit equipment suppliers and service providers in developed countries.

The Second Meeting of ITU-D Study Group 1 and 2 was held in Geneva, Switzerland, from 7-18, September 2015, eWALL, represented by P01, attended and contributed to the ITU-D SG 1 meeting, with a proposal on the effect of network neutrality (NN) on the success of 5G and IoT. NN policy may have a negative effect on 5G wireless due to the emergence of over-the-top services and affect other areas, such as, emergency services provision. eWALL is about delivering personalized services to patients in need, and is interested to have the NN concept well considered in standardisation circles. NN promotes a ‘no blocking’, ‘no throttling’ and ‘no prioritization’ policy. The first two have reached a consensus, but the ‘no prioritization’ policy means that the network providers should not provide differentiated services based on charges of quality of service-QoS (here the difference service means the different service qualities provided by network providers to Internet companies). This has a potential to jeopardize the delivery of emergency services, that should always be prioritized, and to degrade the quality of experience for the eWALL users. Usually, network providers guarantee the QoS of the network in two ways, one is the Resource Reservation Protocol (RSVP) and the second way is Differentiated Service (diffserv). RSVP is a signalling mechanism, which uses integrated services (Intserv) semantics to invoke per-conversation traffic handling. RSVP simply provides a lot of resources with rich and secure equipment and it aims to cope with the expected margin in the “peak” demand. But it is expensive, and cannot cope with the scenario when peak demand is unexpected. Meanwhile, the deployment of additional resources is also time-consuming. Diffserv is an aggregate traffic handling mechanism to address scalability concerns associated with earlier approaches. By listening to RSVP signalling, network devices are more readily able to identify and classify traffic in order to determine the appropriate traffic handling mechanism. But with NN, the differentiated service is banned in the public network. eWALL relies on a sound and always there telecom infrastructure, and therefore, has pushed forward this concern.

3.5 Broadband Commission: Working Group on Health

The Working Group on Health identified opportunities for broadband-based solutions to advance primary health systems and determine the most effective ways to scale them up. The objectives of this body are to identify and target possible partnerships which could result in scale-up initiatives in the Millennium Villages (e.g., in Nigeria); to increase training for Community Health Workers (CHWs) by leveraging ICT and more specifically mobile broadband services.; and to provide a test-bed for quantifying the impact of broadband penetration on social and economic development (and the MDGs).

eWALL has not been participating to these activities but we are monitoring them and plan to disseminate the project outcomes to this group.

3.6 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

Body Area Network – BAN – technology is the use of small, low power wireless devices which can be carried or embedded inside or on the body. Applications include health and wellness monitoring; sports training (e.g. to measure performance); personalized medicine (e.g. heart monitors); personal safety (e.g. fall detection).

A number of wireless BAN communication technologies have been implemented, based on existing radio technologies. But, if BAN technology is to achieve its full potential, there is need for a more specific and dedicated technology, optimized for BAN. For example, solutions for monitoring people during exercise one or two hours a day, a few days a week, may not be suitable for 24/7 monitoring as part of IoT. Such a dedicated BAN technology would need features such as:

- Ultra-low power radio, with a lower complexity Medium Access Control (MAC) protocol for extended autonomy
- Enhanced robustness in the presence of interference
- Interoperability when communicating over heterogeneous networks in the future IoT

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.

TC SmartBAN's scope includes communication media, and associated physical layer, network layer, security, QoS and lawful intercept, and also provision of generic applications and services (e.g. web) for standardisation in the area of BAN technologies. TC SmartBAN continues the activities started by EP eHEALTH to serve as horizontal' nucleus for the co-ordination of ETSI's activities in the Health ICT domain (eHEALTH, mHEALTH, pHEALTH etc.) and to co-ordinate ETSI positions on Health ICT related issues including telemedicine and represent ETSI externally.

TC SmartBAN scope does not include radio matters (HENs for market access) and EMC.

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.

eWALL was invited to join TC SmartBAN in April 2015 to take part in the activities and to contribute to the Draft specification on n the SmartBAN unified data representation formats, semantic and open data model. An example of a Smart BAN end-to-end Architecture considered by the TC Smart BAN is shown in Fig.

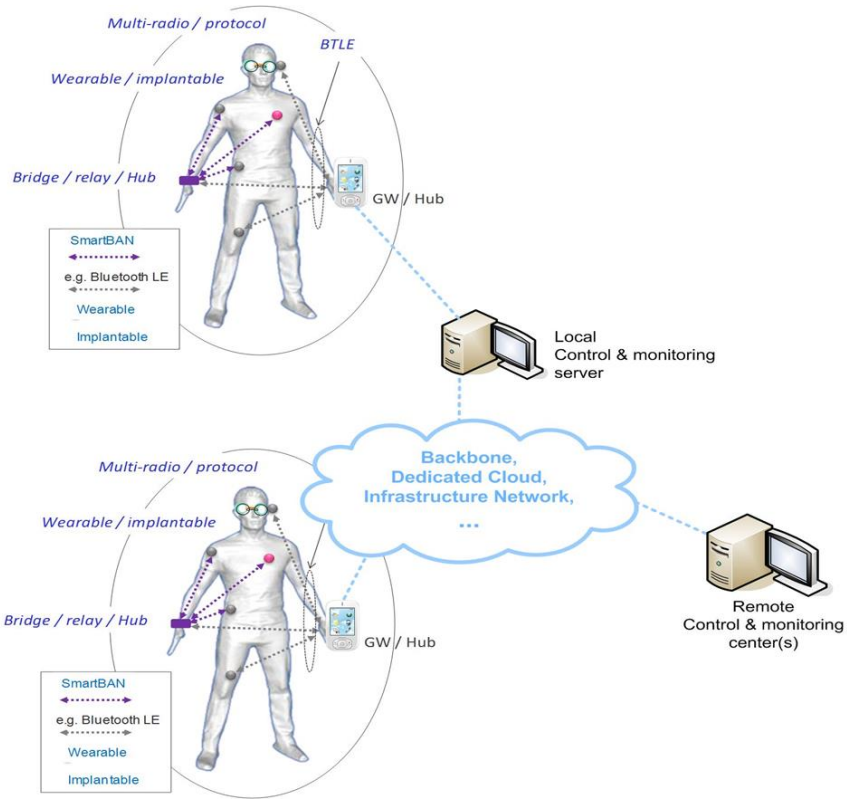

Figure 8 Example of considered SmartBAN end-to-end architecture.

One main objective of Work Item 1.1 is the BAN heterogeneity management through the specification of a generic sensor and sensor data description and transfer format. This description format shall be as rich as possible to allow e.g. conflict resolution or similarity detection, but shall also be handled with low processing, low power and in quasi real time (e.g. latency < 125ms and node addition or removal time < 3s **Fejl! Henvisningskilde ikke fundet.**). In that context, two scenarios shall a priori be envisioned:

- Or the proposed ontology is sufficiently light for allowing the sensor raw data pre-processing within the sensor itself,
- Or the pre-processing is deported to most powerful BAN's nodes. In that case, aforementioned nodes such as the BAN Hub or the BAN coordinator seem a priori good candidates for handling that pre-processing.

eWALL will contribute to the finalization of these items.

5 eWALL Standardization via CEN TC 251

The CEN is the European Committee for Standardisation. The TC (Technical Committee) 251 is responsible for Medical Informatics (Directory of the European Standardisation Requirements for Healthcare Informatics and Telematics). Most of the scopes, drafts, and documents mentioned in the following are available on the WEB server of the CEN/TC 251 addressed by http://miginfo.rug.ac.be:8001/.

A major aspect of medical informatics is the transfer of healthcare information between different computer systems. In order for there to be a meaningful transfer of information, it is necessary for the disparate computer systems to have agreed means of transfer. While there are a number of ad hoc (often proprietary) standards available, it is much easier to achieve full interworking across national boundaries by using internationally agreed standards. In any case, this is a requirement of EC Decision 87/95/EEC. Most of these standards are based on the "Basic Reference Model of Open Systems Interconnection" (ISO/IEC 7498-1:1994).

For various reasons, such standards often have a wide range of options and, although conformance to a specific standard is a necessary condition for interworking, it is not usually a sufficient condition. As a result, it is necessary to select combinations and options within standards which work together to provide a particular end-user function (a "profile"). Profiles themselves can be international standards - International Standardized Profiles (ISPs).

The European Workshop for Open Systems (EWOS) is concerned with the development of profiles for Open Systems Interconnection (OSI) and, more recently, with the more general Open Systems Environment (OSE). The role of its Expert Group on healthcare (EG MED) is to develop appropriate profiles for the healthcare domain and identify requirements for base standards where appropriate standards do not exist.

In many cases, it is expected that these profiles will not differ from those applicable in other contexts. In other cases, specific profiles will be required. Furthermore, there will be international standards which are of particular relevance to healthcare (e.g. ISO/IEC 12087 – “Image processing and interchange") and for which profiles do not exist. Again, EG MED will undertake such profiles.

Thus the principal justification for the work in EWOS/EG MED is to produce profiles for healthcare in order to enable the meaningful transfer of information between distributed healthcare systems.

To analyse the standardisation gaps, Stelar (P12) monitored European standardisation activities related to privacy and data protection carried out by CEN TC251 Health informatics (with which eWALL established a formal Project Liaison earlier).

Moreover, Stelar started to draft preparatory work on the European standardisation proposal concerning a Privacy-by-Design method for the development of eHealth systems and a related so-called standardisation request that could be adopted by the European Commission.

6 Conclusions

eWALL has been very active in all relevant standardisation activities. This will have a two-fold impact, on one side through contributions to standardisation, eWALL will disseminate the project results, which will give it a permanent record, 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 will understand better some possibly critical aspects that can be fed back into the project work.

eWALL will continue to actively contribute to the standardisation activities in the final project year.

Bibliography

[1] “The internet of things” [Online]. Available: http: //www.iot-i.eu/iot/public/news/resources/TheThingsintheInternetofThings_SH.pdf. [Accessed: June-2015].

[2]P. Mahalle, N. R. Prasad, and R. Prasad, “Identity Management Framework towards Internet of Things. CTIF Aalborg, November 2013.

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

[4] Ingo Friese, “Concepts of Identity within the Internet of Things - DG - Identities of Things - Kantara Initiative.” [Online]. Available: http://kantarainitiative.org/confluence/display/IDoT/Concepts+of+Identity+within+the+Internet+of+Things.[Accessed: Jul-2015].

[5]“Final: OpenID Authentication 2.0 - Final.” [Online]. Available: http://openid.net/specs/openid-authentication-2_0.html. [Accessed: May-2015].

[6] M. V. Moreno, J. L. H. Ramos, and A. F. Skarmeta, “User role in IoT-based systems,” 2014 IEEE World Forum on Internet of Things (WF-IoT), pp. 141–146.