Privacy-Preserving Management of Personal Data For Assisted-Living Applications

Gina Kounga, Marco Casassa Mont, Pete Bramhall

HP Laboratories
HPL-2010-200

Keyword(s):

Assisted-living, access control, privacy, consent

Abstract:

The increasing proportion of elderly people in most industrialised countries introduces new challenges. One of these is the provision of efficient and cost-effective caring. Assisted-living solutions use technological tools to allow medical care to be remotely provided to individuals and to provide monitoring capabilities permitting carers and medical authorities to observe and monitor individuals' health states. However, the provision of remote care requires personal data to be collected about individuals with pervasive technologies. Therefore, suitable assisted-living solutions should protect individuals' privacy. In this paper, we propose a solution providing a privacy-aware management of personal data in such scenarios. The proposed solution relies on a communication box, located at the individuals, which automatically protects individuals' privacy based on their consent. It further relies on access control components which guarantees that the entities involved in the provision of remote care always manage individuals' personal data as consented by these individuals.

External Posting Date: December 21, 2010 [Fulltext] Approved for External Publication

Internal Posting Date: December 21, 2010 [Fulltext]

To be published in the Proceedings of 1st International Workshop on the Security of the Internet of Things (SecIoT'10) Tokyo, Japan, December 2010.

Privacy-Preserving Management of Personal Data For Assisted-Living Applications

Gina Kounga
Hewlett-Packard Laboratories
Long Down Avenue
Stoke Gifford
Bristol BS34 8QZ
United Kingdom
Email: Gina.Kounga@hp.com

Marco Casassa Mont
Hewlett-Packard Laboratories
Long Down Avenue
Stoke Gifford
Bristol BS34 8QZ
United Kingdom
Email: Marco.Casassa-Mont@hp.com

Pete Bramhall
Hewlett-Packard Laboratories
Long Down Avenue
Stoke Gifford
Bristol BS34 8QZ
United Kingdom
Email: Pete.Bramhall@hp.com

Abstract—**The increasing proportion of elderly people in most industrialised countries introduces new challenges. One of these is the provision of efficient and cost-effective caring. Assisted-living solutions use technological tools to allow medical care to be remotely provided to individuals and to provide monitoring capabilities permitting carers and medical authorities to observe and monitor individuals' health states. However, the provision of remote care requires personal data to be collected about individuals with pervasive technologies. Therefore, suitable assisted-living solutions should protect individuals' privacy. In this paper, we propose a solution providing a privacy-aware management of personal data in such scenarios. The proposed solution relies on a communication box, located at the individuals, which automatically protects individuals' privacy based on their consent. It further relies on access control components which guarantees that the entities involved in the provision of remote care always manage individuals' personal data as consented by these individuals.**

Index Terms—**Assisted-living, access control, privacy, consent**

I. Introduction

Many industrialised countries have been facing an ageing of their populations [1]. Some consequences of this phenomenon are the increase of age-related diseases such as Alzheimer's disease [2] and the increase of individuals requiring special treatments for chronic diseases. Assisted-living applications [3], [4], [5] are expected to allow individuals to be provided high quality care in the friendly environment of their home. This, by using technologies allowing individuals' health and safety to be remotely monitored by doctors and carers and remote actions assisting these individuals' physical integrity and well-being to be performed. However, remotely monitoring individuals' health and safety means that personally identifiable information (PII) must be distributed to and processed by third parties. In this paper, we define a solution which provides the secure and privacy-preserving management of individuals' PII from their collection by sensing equipments located in individuals' homes to their transmission to and use by third parties. Our solution is designed to guarantee that during the entire lifecycle of personal data, individuals' personal data are only used as consented. For that, our solution relies on a representation of consent discussed by Kounga et al. [6] which, contrary to the opt in/out mechanisms generally used in the literature, provides individuals the freedom to fully specify how they would like to limit their personal data to be used. Consent is represented as a set of fine-grained privacy preferences, specified at the initialisation phase by individuals, that define the actions that are permitted to be performed on a personal data item or a group of personal data items. Later, their consent is automatically and transparently enforced. Here, we describe the mechanisms which guarantee the automatic and privacy-preserving management of individuals' PII as well as those providing the easy and secure setting and management of sensing equipments by individuals and/or carers.

A. Scenario

1) Actors:

Four actors exist in the scenario that we consider in this paper: the data subject, the carer, the trusted authority (TA) and the trusted third party (TTP). The data subject is the individual whose health and safety are being monitored. The carer designates the individual that is responsible for looking after the data subject and that needs to receive the monitored information to take decisions preserving the data subject's health and safety. The TA is an authority, such as the police or an ambulance company, which is trusted to help the data subject in case of emergency and to manage personal data related to an emergency case for the duration of the emergency. Finally, the TTP is an entity, such as an hospital or healthcentre, which is responsible for providing some assisted-living services to the data subject. The TTP needs to receive the monitored data to provide care and safety to the data subject. It is further trusted to manage any sensed PII properly during a time period that can be long.

2) Scenario description:

In order to be provided some assisted-living services, the data subject and her carers first need to register with a TTP. For safety reasons, it may be suitable to require that at least two carers register. One of the carers, the primary carer, will be the one that will have an administrative power allowing it to take some decisions for the data subject when the data subject is unable to take some. Such decisions can for instance be sending PII related to the data subject to the TA in case of emergency. In cases where the primary carer is temporarily unable to fulfill his/her duty, a mechanism (described in Section IV-D) allows that carer to elect a secondary carer as primary carer. After registration has been done, the TTP provides the data subject and her carers with some sensing equipments that they need to position in the data subject's home. They are further provided with a communication box equipped with a wireless (e.g., 802.11 interfaces [7]) network interface. That communication box has the capabilities to manage (i.e., to generate, distribute, securely store and update) cryptographic keys, to manage (collect, securely store and securely distribute) personal data, establish secure communication channels and control access to some critical resources.

The sensing equipments provided by the TTP should have wireless and NFC [8] interfaces to ease their set up. Each of the sensing equipments provided by the TTP has a public key, e.g. a Diffie-Hellman public key [9] and is able to: generate Diffie-Hellman keys, securely store some secret keys, use these secret keys to secure their communications, securely store an identifier and receive and execute the control commands (e.g. store session key, update session key, remove session key, use a specific session key for securing a specific interaction, etc.) received from the authorised communication box. To avoid any unauthorised re-initialisation of the secret keys stored by an equipment, each equipment should only accept to establish one long term secret key and the update of a secret key should only be authorised after the knowledge of that secret key has been proved. Furthermore sensing equipments should be such that, after they have been assigned a long term session key, they should be unable to transmit data in clear.

As assisted-living applications are to be deployed in the future, it is highly probable that new sensing equipments with features – such as those previously specified – that better suit these applications' requirements will have to be introduced. Further, as sensing equipments may be such that they must be carried by the data subjects, there is the need for technologies that do not hamper data subjects' freedom of movement. Wireless technologies provide this.

Finally, the TTP provides the data subject and her carers with some administrators' mobile devices such as some personal data assistants (PDAs) which also have wireless and NFC interfaces. As the carers will need to receive PII about the data subject at anytime to verify that her physical integrity and health status are fine, the wireless interfaces on each administrator's mobile device should allow the device holder to be constantly online. This can be achieved if administrator's devices are connected to mobile telephone networks.

Administrators' mobile devices are equipped with parameters that allow them to access to specific configuration functions of the communication box. They act as a relay gateway when the communication box is unavailable due to some technical problems.When they belong to a primary carer, they allow the secure and privacy-aware transmission of PII to TAs and the election of secondary carers as primary carers.

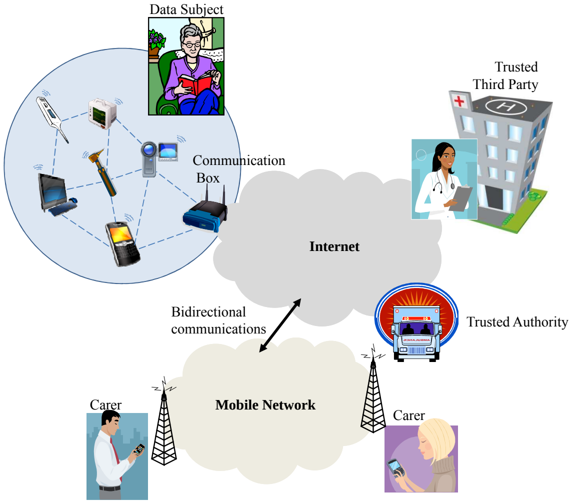

Fig. 1. Data subject's WHAN composed of assisted-living sensing equipments connected to the TTP and the carer

After all the assisted-living sensing equipments have been positioned in the data subject's home, they form a Wireless Home Area Network or WHAN connected to the TTP, the carers and other networks by the communication box, see Figure 1.

The TTP has a specific access control architecture, defined by Kounga et al. [6], that allows it to manage PII received from the data subject's WHAN as specified by the data subject or/and her carers with her preferences. Because of page limitations, this architecture is not discussed.

The TA is equipped with a device in which are installed the same applications as those installed on the administrator's device. This allows the TA to: securely receive messages sent by carers in case of emergency and properly manage the PII contained in these messages.

B. Related Work

Many solutions have been proposed that deal with similar scenarios as the one previously discussed. Wang et al. [3] proposed an open system architecture using an assisted-living hub (ALH) which is similar to the data subject's communication box. This solution does not provide access control management and the management of personal data through the entire sensed PII lifecyle. However, as highlighted by Kotz et al. [10], automated management of personal data allowing data subjects to control how the sensed PII related to them are going to be used by TTPs is an important research issue. May et al. [11] proposed a solution that relies on the architecture specified by Wang et al. and that defines a secure and privacy-preserving transmission protocol for the transmission of data between: the ALH, the assisted-living service provider and the clinician's computer. However, because the security needs of communications may vary depending on their goal as well as the data they contain, setting dynamically the protocol to be used to secure communication – as done by our solution – provides more flexibility. Our solution achieves this.

C. Organisation of the paper

In this paper, we present a solution that allows individuals to easily set up WHANs allowing some TTPs to securely and remotely monitor their health and safety. Our solution further provides individuals with means to control how their personal data are to be used by these TTPs. To achieve the foregoing, our solution extends the approach proposed by Kounga and Prasad [12] to allow the management of personal data.

This paper is organised as follows. In Section II we analyse the requirements of the problem dealt with. Then, in Section III, we present the architecture of the communication box. We detail the operation of our solution in Section IV and discuss our work in Section V. Finally we conclude our paper in Section VI.

II. Requirements

In the previously presented scenario, the interception of exchanged PII may expose data subjects' physical and psychological safety by allowing badly-intentioned people to have enough information to do them harm. As assisted-living applications rely on pervasive technologies such as wireless networks, there is indeed the risk that unauthorised entities manage to eavesdrop the data exchanged in the data subject's WHAN or between the data subject's WHAN and authorised entities (i.e., TTPs, carers and TA). To avoid this, WHANs' communications should be secured. Besides this, to allow the data subject to control the manner in which PII related to her are to be used, mechanisms should be put into place which permit the data subject and/or her carers to define privacy preferences specifying how the PII that are being monitored are permitted to be used by TTPs. When the data subject is unable to define privacy preferences, this task must be performed by the primary carer (see Section IV). Further mechanisms should be put into place which guarantees that these preferences are always enforced on PII received by the TTPs, the TAs and the carers. Because of space limitations we do not describe these mechanisms in this paper. However, these rely on Kounga et al.'s proposal [6]. Finally, as the mechanisms that need to be put into place may be used by individuals without information security knowledge, it is important that these mechanisms be easy to set up and maintain.

III. Architecture

In this section we define the architecture that allows to automatically protect individuals' privacy based on their consent. This architecture is deployed within the communication box provided at initialisation by the TTP to the data subject and her carers. It relies on components allowing:

- Privacy preferences to be systematically bound to each piece of PII being sent outside the WHAN to guarantee that receiving parties will know how they have to limit the use of these PII.
- Security algorithms and protocols to be dynamically selected based on the type of the interactions taking place with or within the WHAN. These algorithms and protocols are then used to secure these interactions.

In order to guarantee that PII generated within the WHAN are only accessed by authorised data as specified by the data subject with her preferences, we use the sticky policy paradigm introduced by Karjoth et al. [13]. In our solution, preferences are cryptographically associated to all the PII items exchanged by authorised entities in such a way that the access to the PII items can only be granted if the conditions specified by the preferences are being fulfilled. Some cryptographic implementations of this paradigm such as those proposed by Casassa Mont et al. [14] and Tang [15] could be used.

A. Overview

The data subject's communication box is responsible for managing the security of communications:

- Between authorised assisted-living sensing equipments within the WHAN;
- From TTPs, or from the carer, to authorised assisted-living sensing equipments within the WHAN;
- From the WHAN to TTPs or the carer.

It is further responsible for providing data subjects with means to control how their PII is to be used by the TTPs and carers. The architecture that permits to provide the foregoing is represented in Figure 2.

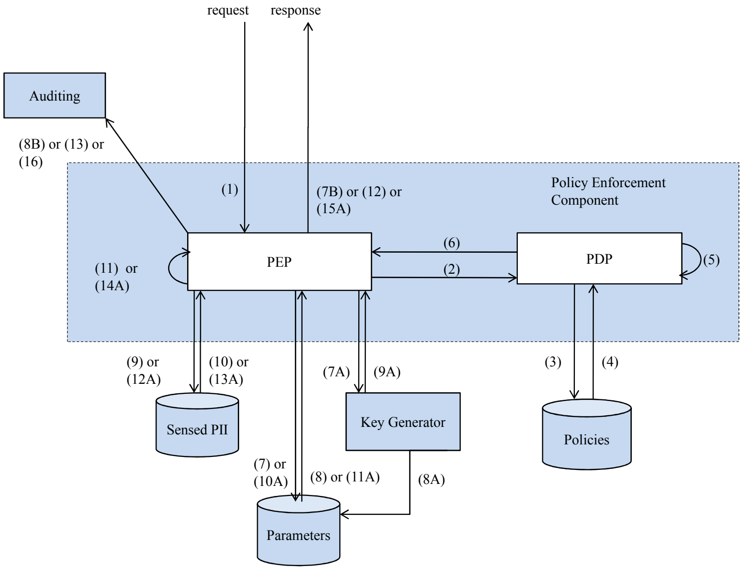

Fig. 2. Architecture of the data subject's communication box

It is composed of a policy enforcement component which relies on the Policy Enforcement Point/Policy Decision Point (PEP/PDP) model [16]. The PEP is responsible for transmitting requests to the PDP and for enforcing decisions returned by the PDP. Two kinds of requests are managed by the PEP:

- *Secure channel requests*: This kind of requests permits a principal – i.e., a unique entity [17] – A to request the establishment of a secure communication channel with another principal B.

- *Data access requests*: This kind of requests permits a principal A to request the access to some data sensed by a specific sensing equipment from the WHAN.

The interactions between components composing the architecture are as follows. An entity that needs a secure communication channel to be established between it and a sensing equipment within the WHAN – or that needs to access some data sensed by an equipment from the WHAN – sends a request to the PEP (see (1) in Figure 2). After receiving the request, the PEP transmits it to the PDP (see (2) in Figure 2). The PDP then extracts the suitable policy from the policies database (see (3) and (4)) and evaluates it (see (5)). After it has been done, the PDP returns an authorisation decision to the PEP (see (6)). This authorisation decision can be *permit*, if the access has been granted by the PDP, or *deny*, if it has not.

If the decision is *deny*, then the PEP returns the received response to the requesting entity (see (7B)). If the response is *permit*, two cases have to be considered:

1) The action authorised by the PDP requires some new cryptographic material to be generated;
2) The action authorised by the PDP does not require any new cryptographic material to be generated.

In the case 1, the PEP sends a request to the Key Generator to generate the required cryptographic material (see (7A)). After having received it, the Key Generator first generates the requested cryptographic material and then creates an new entry in the parameters database for this material (see (8A)). The Key Generator finally sends a confirmation to the PEP that the cryptographic material has been created (see (9A)). After receiving the confirmation, the PEP can extract that material from the parameters database as well as the suitable sensed PII from the Sensed PII database (see green (10A) to (13A)) before formatting a response (see (14A)) and sending it to the requesting entity (see (15A)).

After a response has been returned by the PEP, the initial request, the PDP decision and the response sent to the requester are sent to the Auditing component in order these to be logged (see (8B), (13) and (16)).

In the case 2, the interactions are similar as in the case 1, except that no interaction with the Key Generator is required.

B. Policies Database

The policies database stores all the policies the PDP relies on to evaluate a request. These policies are defined by each TTP to avoid the risk that inappropriate policies be used by a communication box. These policies are of different types. Administration policies, for instance, define how the data subject's communication box have to interact with the TTP for maintenance purposes. Among the different policies, some need to be assigned by the WHAN administrator to each sensing equipment. Each of these later type of policies defines the security services that are to be provided to secure the communications and the accesses to the PII respectively established by and sensed by the sensing equipments participating in the WHAN. Each policy is associated to a level. There could be as many levels, and therefore as many policies, as different sets of security services to be provided. The same levels and policies are specified within all the data subjects' communication boxes provided by the TTP. This approach is interesting because it does not require data subjects and carers to understand the technical policies but only to understand how the communications will be protected if a level is chosen. The provision, by the TTP to the data subject and the carers, of an illustrated documentation explaining simply the later may allow to achieve this.

Each policy should at least specify:

- The security services to be provided to communications established by the sensing equipment which the policy is assigned to;
- The protocols and algorithms to be used to provide these security services;
- The type of interactions the sensing equipment is authorised to have. These can be of the following types:
  - *Internal only*: specifies that sensing equipments to which the policy apply must only communicate with authorised entities within the WHAN;
  - *Internal and external*: specifies that sensing equipments to which the policy apply can communicate with authorised entities within and outside the WHAN;
- Obligations. Different types of obligations should be managed. A first type should allow the management of the cryptographic material used to secure the communication by specifying, among others, the duration after which the cryptographic material must be updated. Another type should specify constraints about how data should be managed by the communication box beyond access control or security [18]. Such obligations may for instance specify that after a week PII that have not been accessed should be removed.

To guarantee the integrity of policies, these are digitally signed by the TTP that wrote them.

C. Key Generator

The Key Generator is responsible for generating the cryptographic material to be used to secure communications. It receives from the PEP some parameters that specify the algorithms to be used to generate the required material. Because these parameters must be specified within the policies, they must be extracted by the PDP from evaluated policies and returned to the PEP.

D. Parameters and PII Databases

The parameters database specifies, for each sensing equipment composing the WHAN, the parameters that need to be used by the PEP to enforce the PDP's decision. This database contains at least the following elements for each sensing equipment whose interactions have to be secured by the communication box: the sensing equipment's identifier, the sensing equipment's long-term secret key, the access control list (ACL) containing the identifiers of entities the equipment is authorised to communicate with, (for each of the entities within the ACL) the associated session key and the data subject's preferences to be associated to the PII sensed by the equipment. These preferences define how the sensed PII data must be used by authorised entitites. To guarantee that cryptographic keys are securely stored within the database, they are encrypted with the communication box's public key.

The sensed PII database stores all the PII sensed by sensing equipment participating in the WHAN. Its design must allow to identify the TTPs which provided sensing equipments having generated the stored PII. As for the parameters database, sensed PII in the database are encrypted with the communication box's public key.

E. Auditing

The Auditing component records the communication box's activity to allow third parties, such as forensic investigators called in after a serious incident or apparent failure, to investigate whether the communication box behaved properly. Records stored by the component should be associated with non-repudiable proofs of their authenticity to allow any forensic analysis to establish their validity. Like other PII stored in the communication box, the records should be securely stored. The technology used to securely store them, should allow third parties to access these records even if the data subject is not available. But at the same time, it should not allow the TTP to access to the records to avoid the risk that someone at the TTP accesses the records and modify them to protect his interests. Threshold cryptography [19] can allow the previous. The auditing box could indeed encrypt the records with a public key whose corresponding private key could be separated within n shares. One of these could then be distributed to the TTP and each of the carers. Shares should be such that the private key could be recomposed based on any two shares. Default policies installed on carers devices and at the TTP should specify that the share can only be sent to forensic investigators after a valid share request was received from them.

F. Alternative approach

Here, we have considered that all the previously described components are embedded in the communication box. However, an alternative approach can be to have few components within the box and other at a different location, such as a server. This later approach would allow to extend the capabilities of boxes already provided in the market to adapt them to our scenario. Either of the approaches suits our solution.

IV. Solution

Our solution comprises a first phase during which the data subject and/or her primary carer use(s) a dedicated application on their administrator's device to securely set the WHAN and specify how the sensed PII should be managed as well as the access rights. These parameters are then securely sent to the communication box. Afterwards, the communication box can operate independently of the data subject to provide the privacy-aware management of the PII related to her and to secure communications with and within the WHAN. To automatically manage technical problems that could appear at the communication box, the TTP provides online technical support and if the communication box must be collected by the TTP's technical team in order it to be repaired, mechanisms are automatically put into place to make the data subject's administrator's device temporarily behave as a communication box.

A. Registration

At registration, the data subject and her carer(s) have to specify who will have the right to administer the WHAN. Then, each specified administrator is provided with an administrator's mobile device that contains a smartcard with some cryptographic materials[1] allowing it to securely communicate. Each administrator's device is further equipped with an application permitting to configure the communication box. The application should be intuitive enough to allow non-experts to easily and efficiently do the configuration. It should have password-protected functionalities to guarantee that only the suitable entity can access them. The communication box is also equipped with a smartcard with similar cryptographic material[2].

B. Initialisation

Initialisation comprises the following three steps: (1) the establishment of long-term secret keys with and the distribution of identifiers (IDs) to the assisted-living sensing equipments composing the WHAN, (2) the specification of the policies to be used to secure sensing equipments' communications and access to sensed PII as well as the specifications of the data subject's consent through the setting of privacy preferences to be applied to sensed PII and (3) the transmission of the configuration parameters to the communication box. In the remainder of this section we present these steps.

1) Establishment of long-term secret keys:

To securely establish long-term secrets with, and distribute identifiers to, assisted-living sensing equipments, the approach introduced by Stajano in [20] is used: a physical contact between the devices that have to negotiate the long-term secret

[1] its public/private key pair that allows the device to establish secure communication channels, the communication box's public key that allows the administrator's device to authenticate the communication box, the TTP's public key that allows the administrator's device to establish secure communication channels with the TTP and the trusted authority's (authorities') public key.

[2] a public/private key pair that allows the communication box to establish secure communication channels, each administrator's public key that allows authenticating the devices that are authorised to configure the communication box, the TTP's public key: It allows the communication box to establish secure communication channels with the TTP and the trusted authority's (authorities') public key.

key is established. For that, the administrator must first run the configuration application on her device and activate the right menu. The application then generates a unique identifier ID_{E1} and a Diffie-Hellman public key g^{K}. Then, the administrator establishes a contact between her device and $E1$ the assisted-living sensing equipment which a long-term secret key must be established with. This contact allows $E1$ to send its Diffie-Hellman public key $g^{K_{E1}}$ to the administrator's device and the administrator's device to send g^{K} and ID_{E1} to $E1$. After it has been done, both devices generate their shared long-term secret key $LK1$.

As studied by Haselsteiner and Breitfu in [21], even if NFC interfaces are very short ranges, some active attacks are still possible but very hard in the suitable setting. Therefore, the TTP must provide the administrator(s) with clear guidelines to reduce the risk of such attacks. A passive attack, such as eavesdropping is possible in a distance of few meters from the devices [21]. However, as the Diffie-Hellman key agreement protocol is used, the eavesdropper is only able to know the value of the shared secret if he already knows one of the private keys associated to the public keys exchanged by the administrator's device and $E1$. As the private keys K_{E1} is securely stored by $E1$ – as discussed in Section I-A– it cannot be known by any other entity. Besides this, the private key K associated to the Diffie-Hellman public key generated by the administrator's device is securely stored encrypted with the device's public key. It is only decrypted after the administrator has entered her passphrase and immediately re-encrypted after it has been used. Therefore, any entity that does not know the administrator's passphrase cannot know the private key. Besides this, after the initial establishment of the long-term secret key, no other entity than the administrator's device is able to update $E1$'s long-term secret key. The foregoing makes eavesdropping attacks hard to succeed.

2) Policy and parameters specifications:

After the establishment of the long-term secret key, the administrator uses the configuration application on her device to assign a policy to $E1$. This policy is to be chosen among the set of policies predefined by the TTP and available for selection in the configuration application. The selection of the policies is made based on the level associated to each policy. Besides the specifications of the policies, the administrator uses the same application to specify the following parameters to be assigned to $E1$ in the parameters database: the privay preferences that will apply to PII sensed by $E1$, the ACL associated to $E1$, the TTP[3] which issued $E1$.

3) Transmission of the configuration parameters to the communication box:

Once the required parameters have been set, the administrator uses the configuration application on her device to establish a secure communication channel with her communication box using the public keys pre-installed on her device's smartcard. This can be achieved with different protocols such as Transport Layer Security [22]. Then, the device sends $E1$'s configuration parameters to the communication box. After the communication box has received them, it adds an entry for $E1$ into its parameters database. The parameters are only stored by the communication box if they have been sent by an authorised administrator's device, i.e., a device whose currently valid public key is stored in the smartcard of the data subject's communication box.

C. Solution's operation

In this section we describe the operation of our solution.

1) Communication between equipments and transmission of sensed PII:

When a sensing equipment $E1$ wants to establish a secure communication with an equipment $E2$, it sends an authenticated secure channel request to the communication box. Then, the authorisation process described in Section III-A is run. The PEP transmits the request to the PDP which verifies its authenticity before evaluating it. This evaluation includes verifying that $E2$ is in $E1$'s ACL and that $E1$ and $E2$ have been provided by the same TTP. $E1$'s ACL and the information about whether or not $E1$ and $E2$ have been provided by the same TTP can be added into the request transmitted by to the PDP by the PEP. If it is the case, the PEP also needs to insert into the request a proof that the added parameters are authentic. Then, if $E1$ and $E2$ have been authorised to communicate by the PDP, the PEP sends both entities a session key through some secure communication channels. The session key is also securely stored in the parameters database (see Section III-D) at the entries associated to $E1$ and $E2$.

When a sensing equipment $E1$ wants to communicate with an entity $E3$ outside the WHAN, or when $E3$ sends a request to the communication box to communicate with $E1$, the same mechanism applies except that the evaluation also consist in verifying that $E1$ is authorised to establish communications with devices outside the WHAN.

In the case where entities insides or outside the WHAN are requesting access to some sensed PII stored by the communication box, the previously described authorisation process is once again run.

Some sensed PII may have to be sent regularly to some entities (e.g. localisation data sent to the carer to protect the safety of data subjects suffering from Alzheimer disease). Therefore, the equipment sensing the needed data will have to be assigned a policy specifying obligations stating that PII sensed by the equipment have to be regularly sent to the carer. Then, the PEP within the data subject's communication box is responsible for enforcing these obligations by regularly extracting the data sensed by the equipment as well as the associated preferences from the Sensed PII database before sending them to the carer's device.

In a case of emergency, the carer uses its administrator's device to run an emergency application. This application then securely sends a pre-defined set of PII, sensed within the data subject's WHAN, to some trusted authorities along with

[3] TTPs may be selected among a list of TTPs provided by the configuration application.

some preferences. These preferences are such that they only authorise the use of the transmitted PII for the duration of the emergency. As the trusted authorities are equipped with devices that run the same applications as those running on the administrator's device, the trusted authorities are able to enforce the preferences.

2) Removing an equipment from the WHAN:

When, for any reason, an equipment $E1$ must temporarily not participate to the WHAN anymore, the administrator uses the configuration application on her device to request the communication box to remove $E1$ from the WHAN. For that, the communication box clears $E1$'s ACL. It further clears the type of interactions that $E1$ is authorised to have. Finally, the communication box requests the entities which shared some session keys with $E1$ to remove them, before clearing these session keys from the parameters database. Then, because no ACL is anymore associated to $E1$, $E1$ cannot anymore participate to the WHAN. $E1$'s long-term secret key is not removed from the parameters database for the following reasons. First, even if $E1$ is not part of the WHAN anymore, it may still be able to transmit sensed PII[4]. By making $E1$ keep its long term secret key, one can guarantee that no other entity than the communication box is able to read the PII transmitted by $E1$. Second, if the administrator later wishes to make the equipment re-participate to the WHAN, the configuration is simplified. However, if $E1$ must permanently be removed from the WHAN, the communication box further requests $E1$ to remove its long term secret key and clears it from the parameters database.

D. Maintenance

a) Management of technical problems:

The TTP regularly verifies the state of the data subject's communication box in order to guarantee that it operates properly. The data subject's communication box also regularly backs up the state of the parameters database on a server located at the TTP. The back up is encrypted with a secret key itself encrypted with the public key of the data subject's communication box and with each of the administrator's devices' public keys. It guarantees that the TTP is not able to know the parameters used by the data subject's communication box. The encrypted secret keys are also stored on a server located at the TTP. In case where a technical problem is detected at the data subject's communication box which requires the communication box to be collected by the TTP's technical team in order the box to be repaired, the TTP sends the encrypted back-up as well as the suitable encrypted secret key to the data subject administrator's device[5]. The data subject administrator's device then temporarily acts as a communication box. This is allowed by a specific application in the device. After the communication box has been repaired, the TTP informs the device that it must stop acting as the communication box. The device can then remove the parameters database.

b) Management of primary carers:

It may happen that, temporarily, the primary carer is not able to fulfill her duty anymore. To manage this case, at registration, the data subject and/or her primary carer are/is requested to specify eligible secondary carers which she could transfer her duty to[6]. Then, when the primary carer activates the application allowing her duty to be transfered, it is indeed only transfered to the elected secondary carer if this one is among those specified at registration. To manage the case where the primary carer may not be able to fulfil her duty for a long term, an ordered list of secondary carers that could be selected to be primary carer should be specified at registration. Then, the similar mechanism as previously discussed allows the primary carer to choose one of the secondary carers within this list to become primary carer. When the initial primary carer is able again to fulfil her duty, she uses the application on her device to send a message to the TTP that then re-establishes her as the primary carer. This activates specific access rights for the new primary carers and deactivates these for the previous one. However, if after a long time, the primary carer has not requested to be re-established as primary carer, the TTP automatically makes the first secondary carer within the provided ordered list become primary carer. If the first secondary carer within the list is not reachable, the second one is tried. This goes on until a secondary carer from the list is found that can become primary carer.

V. Discussion

In this section, we discuss how the proposed solution fulfils the requirements of Section II.

Unauthorised access to PII sensed in the WHAN. In our solution, data access requests must be authenticated to allow the authentication of their sources. Requests are further evaluated by the PDP based on policies assigned by the data subject and/or her carer. After the access is granted by the PDP the PEP encrypts the PII with a key only accessible by the authorised request originator. Therefore, the solution proposed in this paper guarantees that only authorised entities can access to PII sensed in the WHAN.

Restriction of communications to authorised entities. Here, only entities that do have a long-term secret key stored in the data subject's communication box are able to participate to the WHAN. As the establishment of long-term secret keys with sensing equipments as well as their transmission to the communication box are controlled by the administrator and are achieved through secure communication channels, only the entities chosen by the administrator can have valid long-term secret keys. Among these entities, only those that mutually appear on their ACL can receive a session key allowing them to communicate.

Ease of configuration and maintenance. The configuration of

[4] It is important to note that if the communication box received some PII from $E1$ after the administrator has requested to remove it from the network, this PII is discarded.

[5] When the parameters database is stored by the administrator's device, the secret keys it contains are encrypted with the device's public key.

[6] The TTP should verify that the eligible secondary carers are capable of taking decisions for the data subject.

the WHAN is done through an intuitive application run on the administrator's device. Policies are graphically illustrated to show the administrator how they protect communications and accesses to sensed PII. Each policy is identified by a level to allow the association of a level to a set of illustrated security mechanisms. Maintenance of the data subject's communication box is made online by the TTP. In case where the data subject's communication box has to be collected in order to be repaired by the TTP's technical team, a mechanism allows to make an administrator's device temporarily act as the communication box. This guarantees that the data subject can always be provided assisted-living services. This is important as such services may need to be provided on a continuous basis to guarantee the data subject's physical and health integrity.

Specification of use of PII. Data to be sent by the communication box to the carers are associated to the preferences that apply to them before being sent. The application running on the administrator's device then guarantees that these PII are used as specified by the preferences. When, in case of emergency, the carer must transmit some received PII to a trusted authority, the application on the carer's device associates some preferences to the PII before sending them. These preferences specify that the transmitted PII can only be used by the TA for the management of the emergency. Beside this, TAs are equipped with devices running the same applications as the carer's device, the previous preferences can be enforced.

VI. Conclusion

In this paper, we have proposed a solution for assisted-living applications which automatically protect individuals' privacy based on their consent. The solution relies on a communication box, located in individuals' home, to secure: (1) the access to PII that is sensed by assisted-living sensing equipments positioned in individuals' home as well as (2) the communications established between assisted-living sensing equipments and authorised entities such as hospitals and carers' devices. To achieve the foregoing, the communication box relies on security parameters securely distributed by individuals thanks to a administrator device equipped with a specific and intuitive configuration application. The communication box is maintained online by a trusted third party (TTP). In case where it needs to be collected by the TTP's technical team, some mechanisms allow a trusted device to temporarily act as a replacement communication box. This makes maintenance transparent to the individuals and guarantees that individuals can continuously be provided assisted-living services. Finally, our solution allows individuals to define how their personal data are to be used by the TTPs which provide them some assisted-living services. The solution proposed in this paper is being implemented in the context of the British EnCoRe Project [23]. The future work will consist in evaluating this solution and extending it to cover, among others, compliance with data protection laws.

References

[1] United Nations, "World Population Ageing 2009." [Online]. Available: http://www.un.org/esa/population/publications/WPA2009/WPA2009_WorkingPaper.pdf

[2] T. Iwatsubo, Y. Ihara, and I. Kanazawa, "Alzheimer disease research in japan: public funding," *Nature Medicine*, vol. 12, pp. 778 – 779, 2006.

[3] Q. Wang, W. Shin, X. Liu, Z. Zeng, C. Oh, B. K. Alshebli, M. Caccamo, C. A. Gunter, E. Gunter, J. Hou, K. Karahalios, and L. Sha, "I-living: An open system architecture for assisted living," in *In IEEE International Conference on Systems, Man, and Cybernetics*, 2006.

[4] M. Layouni, K. Verslype, M. T. Sandikkaya, B. Decker, and H. Vangheluwe, "Privacy-preserving telemonitoring for ehealth," in *Proceedings of the 23rd Annual IFIP WG 11.3 Working Conference on Data and Applications Security XXIII*. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 95–110.

[5] J. M. Corchado, J. Bajo, Y. de Paz, and D. I. Tapia, "Intelligent environment for monitoring alzheimer patients, agent technology for health care," *Decis. Support Syst.*, vol. 44, no. 2, pp. 382–396, 2008.

[6] G. Kounga, M. Casassa Mont, and P. Bramhall, "Extending xacml access control architecture for allowing preference-based authorisation," in *TrustBus*, 2010, pp. 153–164.

[7] Institute of Electrical and Electronics Engineers, "Ieee 802.11, in first edition 1999-00-00, information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - part11: Wireless lan medium access control (mac) and physical layer (phy) specifications," *IEEE*, 1999.

[8] International Organisation for Standardisation, *Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1)*, Std. ISO/IEC 18 092:2004, 2007.

[9] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

[10] D. Kotz, S. Avancha, and A. Baxi, "A privacy framework for mobile health and home-care systems," in *SPIMACS '09: Proceedings of the first ACM workshop on Security and privacy in medical and home-care systems*. New York, NY, USA: ACM, 2009, pp. 1–12.

[11] M. J. May, W. Shin, C. A. Gunter, and I. Lee, "Securing the drop-box architecture for assisted living," in *FMSE '06: Proceedings of the fourth ACM workshop on Formal methods in security*. New York, NY, USA: ACM, 2006, pp. 1–12.

[12] G. Kounga and A. Prasad, "Method and apparatus for operating wireless home area networks," *European Patent EP 1993301*, July 2009.

[13] G. Karjoth, M. Schunter, and M. Waidner, "Platform for enterprise privacy practices: Privacy-enabled management of customer data," in *Privacy Enhancing Technologies*, 2002, pp. 69–84.

[14] M. Casassa Mont, S. Pearson, and P. Bramhall, "Towards accountable management of identity and privacy: Sticky policies and enforceable tracing services." IEEE Computer Society, 2003, pp. 377–382.

[15] Q. Tang, "On using encryption techniques to enhance sticky policies enforcement," http://eprints.eemcs.utwente.nl/14262/, Enschede, Technical Report TR-CTIT-08-64, 2008.

[16] R. Yavatkar, D. Pendarakis, and R. Guerin, "A Framework for Policy-based Admission Control," RFC 2753 (Informational), Internet Engineering Task Force, Jan. 2000.

[17] M. Bishop, *Computer Security: Art and Science*. Addison-Wesley, 2003.

[18] M. Casassa Mont and F. Beato, "On parametric obligation policies: Enabling privacy-aware information lifecycle management in enterprises," in *POLICY '07: Proceedings of the Eighth IEEE International Workshop on Policies for Distributed Systems and Networks*. Washington, DC, USA: IEEE Computer Society, 2007, pp. 51–55.

[19] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[20] F. Stajano, "The resurrecting duckling - what next?" in *Revised Papers from the 8th International Workshop on Security Protocols*. London, UK: Springer-Verlag, 2001, pp. 204–214.

[21] K. Haselsteiner and K. Breitfuß, "Security in near field communication: Strengths and weaknesses," April 2006.

[22] T. Dierks and E. Rescorla, "The TLS Protocol Version 1.1," RFC 4346 (Proposed Standard), 2006.

[23] EnCoRe Project, "Encore project website." [Online]. Available: http://www.encore-project.info/