Data Protection in Elderly Health Care Platforms

Angelo Costa[1], Aliaksandra Yelshyna[2], Teresa C. Moreira[2], Francisco C.P. Andrade[2], Vicente Julián[3], Paulo Novais[1]

[1] Centro ALGORITMI/Departamento de Informática, Escola de Engenharia, Universidade do Minho, Portugal [acosta, pjon]@di.uminho.pt

[2] School of Law, University of Minho yelshyna@gmail.com, [tmoreira, fandrade]@direito.uminho.pt

[3] Departamento de Sistemas Informáticos y Computación, Universitat Politècnica de València, Valencia, Spain vinglada@dsic.upv.es

Abstract The protection of the citizens digital identity is crucial on the current technological age. Computational systems menace the privacy of the users by sharing their information to others and by keeping, and sometimes monetizing, it indefinitely. The issue is that to obtain the positive effects of the computational systems the users have to relinquish their personal information. Ambient Assisted Living (AAL) systems thrive on data from the users to provide personalised assistance. AAL focuses on creating tools for elderly people according to their medical condition, thus requiring access to personal and private information. Most of the projects have unsupervised data processing and cross-share personal information. In this paper it is used the iGenda project, which is a Cognitive Assistant inserted in the AAL area, to expose the current legal limitations that can be extrapolated to most AAL projects. It also presents the principles and legal guarantees of data protection and transmission, legal aspects, and how can they be implemented on these systems containing features that may be a threat.

Keywords: Healthcare Platform, Ambient Assisted Living, Data Protection, Privacy, iGenda

1 Introduction

According to the UN report [18], in the year 2050 the elderly population is expected to be over 2 billion. This growth of human longevity and birth rate decrease is threatening the sustainability of health systems and forces to rethink health care planning and provision [19].

Furthermore an important issue is the great medical care that the elderly population needs. Currently there are efforts to provide technological solutions through the use of AAL developments that provide medical assistance through the use of devices and services that connect them with medical staff [7,11,12,16,20]. The AAL aims at people with some sort of disabilities, most of the frameworks target the elderly population.

Related Projects In terms of related projects, we can refer three as being ones that fit well the previous description: the AAL4ALL [15], the Care4Balance [1], and the RelaxedCare [13]. AAL4ALL has presented new ways of communicating with heterogeneous devices and services using the IEEE 11073 and the HL7 as base standards, which are commonly used in the medical area. Care4Balance presented a new perspective in terms of gathering information of the caregiver and care-receiver. RelaxedCare aims to create a novel social network that connects its platform users with their relatives.

Medical Devices Medical devices are tested and certified to achieve a high level of protection for human health and safety and a good functioning without any harm or malpractice to its users (Directives 90/385/EEC, 93/42/EEC and 98/79/EC). Therefore, they are very restricted in terms of features and the type of information the possess or generate. This forces the medical devices to be simple and contain only a small amount of information. Consequently, most of these devices is very specialised, thus only performing one operation. AAL projects usually require complete information about the users because most of the features rely on it.

Legal Issues The use of the AAL systems may present some difficult issues from a legal point of view due to the monitoring procedures and the cross-sharing of sensible information; they intend a serious risk of privacy loss. AAL4AAL made an effort to create a standard that encompasses the exigencies that AAL projects require, this would allow them to be legally equivalent to medical devices. Until now there are no advances in this field, as a result, AAL projects have been barred the access to the medical environment. Although this shows a bleak future, it did not stop the development of the projects hoping that the regulations change.

Field tests performed on these projects, and others, reveal that there is a generalized acceptance by the elderly population and by the medical staff. The successful results show that these type of projects are needed and there is a market for them. The main problem relies on the privacy and data protection. There are some procedures to keep data secure, like enforcing encryption and social tools, but they come with a high cost of implementation, maintenance and compatibility.

Encryption One approach of attempted encryption is introduced by Doukas et al. [6], which proposes the introduction of Public Key Infrastructure (PKI) encryption [17] on sensor gateways, disabling middle-man attacks and packet sniffing. This security level is appropriate to secure remote data transmission, where data has to pass several internet nodes but it has a high computational cost. This is unfeasible to be implemented in internal data exchanges. The number of connections established in just one second rely on fast response, thus the overhead required is impractical. Furthermore, the complexity of AAL systems communications exceed the peer-to-peer type, which would require multiple keys to each user, increasing substantially the complexity of the encryption/decryption process.

This paper presents a discussion of the dichotomy between the current legal framework and ALL technology using the iGenda as an example, focusing on the privacy and data protection concerns. The aim is to highlight the issues and recommend possible solutions to harmonize the technological advances and data protection requirements for current and future laws.

In section 2 it is going to be presented an AAL platform, iGenda, showing the data transferred and user access to it. In section 3 it is presented the current data protection framework and the legal warranties related to the AAL action area. Section 4 explains legal aspects of data storage and access law procedures. Section 5 explains the technological implementation challenges. And finally, section 6 presents the conclusions of the paper.

2 The iGenda Example

The AAL and AmI aim to build safe environments that adapt themselves to one's individual needs. Typically used in home environments (that can be adapted to nursing homes and others alike) AAL platforms are built with cost in mind, thus resorting to commercially available devices and software to implement their features. The goal is to deliver medical assistance to one's home, therefore decreasing hospital stays and visits sustaining the familiar feeling that a home provides.

The use of AAL systems require a large amount of personal information about the users of those systems, such as personal health record, data about social contacts, domestic activities, and physical location.

To better demonstrate the AAL concept we present the iGenda project [4,5,10] that is an AAL platform that uses mobile devices and sensor systems to collect and process vital data, displaying them via mobile devices or the iGenda administration web-page. These procedures aim to improve the well-being of the users (the care-receivers) by creating a compendium of health data that can help to identify health problems or critical events.

In terms of features, the iGenda primary feature is to be a communication platform with an calendar manager that intelligently schedules regular events, plans social events and, directed to the medical staff, schedules medical appointments with the care-receivers, facilitating the creation of shared events.

There are three major actors in iGenda: the care-receivers (elderly or mentally impaired people), the caregivers (physicians or family/relatives), and the relatives (family and friends). They have access to specific information tailored to them, according to their needs. For instance, the care-receivers have no need to receive extensive medical information as it would only confuse them.

Apart from these three actors there is also the technician who is a trained professional responsible for the iGenda system and who is bound by a contract.

iGenda relies on data, in fact, without a large amount of data about its users it will not operate correctly. The platform uses a profiling method based on likes and dislikes of the users so it can suggest activities that please them. Thereon, the platform can schedule shared events of leisure activities that please all the participants and that also comply with the active-aging objective.

To find activities that are pleasant to all of the users, the system searches their activities database for similar events. The events have their own ontology, which relies on well-defined tags to each activity. Therefore, all activities are described the same way and their introduction is done by a iGenda technician. The similar activities are ranked by a weighted algorithm that analyses each activity classification (according to each user) and produces a new classification. The higher classified activity is then scheduled in a timeframe common to all participants (that anyone has no activities). For instance, if 4 users (that know eachother) like playing cards and have the Monday afternoon free the iGenda is able to schedule a card game on that time period.

Furthermore, the caregivers have the responsibility to care for the care-receivers that are assigned to them (they can be formal or informal, such as relatives or friends) and receive extended health or personal information about each care-receiver, effectively entering the private sphere of each user.

One of the great privacy protection issue is that in iGenda (and in most of the AAL projects) the information is shared and viewed by several users, some are bound by confidentiality obligations and others are not. Furthermore, the information will be present in iGenda as long as possible, e.g., at least as a specific user is registered in the system but in may be present for a longer period. These choices were taken so the platform is able to relate all information and social connections, thus being able to provide accurate event suggestions and health reports that are grounded to the common medical history.

3 The Data Protection Framework for AAL Systems

European Union legislation on personal data protection is presented by the Directive 95/46/EC (Personal Data Protection Directive) that was adapted in Portugal by the Law 67/98, 26 October on Data Protection (Portuguese Data Protection Act) and Directive 2002/58/EC (Directive on Privacy and Electronic Communications). The currently applicable Directive 95/46/EC is being revised and in the near future will be replaced by the General Data Protection Regulation (GDPR) which establishes rules adapted to the digital era and aims to harmonize data protection rules in the EU, introducing some new principles of data protection: data protection by default and data protection by design, which will then guarantee that data protection safeguards are being incorporated in all planning phases of development of the AAL solutions.

iGenda (and AAL platforms in general) collect and process personal and health data which is particularly sensitive and therefore requires special protection in accordance with the Directive 95/46/CE and Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention N.º 108). In Portugal, article 35 of the Portuguese Constitution stipulates a general prohibition of processing personal data, forbidding the use of informatics for the treatment of data concerning the private life of the citizens [9]. On the other hand, both the Portuguese Law 67/98 and the Directive 95/46/CE have specified that, within the prohibition of processing sensitive data, in addition to all data concerning the private life of the citizens, health, sexual and genetic data must be also included. However, there is an obvious exception to this general prohibition: the case when the data subject expressly consents, through free informed will, without any kind of coercion, being totally aware of all the effects arising out of his/her manifestation of will [2].This requirement of a free and express consent is obviously related with the legal principles of personal data protection. First of all, the principle of transparency, meaning that the person responsible for the data collection and processing must be clearly identified and the data subject must be informed on its purpose and also on the delays for keeping the data, as well as the possibility and conditions of its communication to third parties.

One of the this principles that constitutes the truly fundamental and main principle of data protection is the limitation principle or purpose principle (partially embodied in article 6°, n. 1, paragraph b) of the Directive and in article 5°, n. 1, paragraph b) of the Portuguese Law 67/98). The referred principle prohibits further processing that is incompatible with the original purpose(s) of the collection. Personal and health data collected via AAL should only be processed for the purpose of providing AAL services and should not be used for any way incompatible with those purposes.

Article 6° of the Directive and article 5°, n. 1, paragraph c) of the Portuguese Law 67/98 incorporate this principle of proportionality by stating that personal data must be adequate, relevant, and not excessive in relation to the intended and legitimate purposes for which personal data are collected and/or processed. Also, the processing of personal data must be strictly limited to the minimum required to achieve the AAL objectives, according to the minimization principle. In addition, each consultation of personal data that is available through the AAL should be justified by a real necessity of providing care, treatment or medicine prescription.

The proportionality principle is associated to the quality of the personal data which imposes personal data to be pertinent, kept up-to-date and not excessive in relation to the purpose for which they are collected. The treatment of personal data can only take place when it is indispensable for the initial purpose and irrelevant data should not be collected (article 6°, n. 1, paragraph c) of the Directive).

According to the retention principle the collected data should not be retained in these systems for longer than necessary (see article 6°, n. 1, paragraph e) of the Directive 95/46/CE and article 5°, n. 1, paragraph e) of the Portuguese Law 67/98). This is an ambiguous principle as the maximum time is not defined and can be abused. This principle is established to prevent abuses and enforce legal protection if abuses are done. In the case of AAL projects, and in iGenda, some features require the collected data to be permanent, and that constitutes an abuse of privacy. Therefore, this issue is more relatable to ethical concerns, as while it is not illegal to keep the information a large period of time it may be considered unethical because users may not be aware of such time period. It is hard to fathom the concept of “forever” and what it means, thus most people cannot make an informed decision about the data their are surrendering.

In AAL platforms the care-receiver has the right to access and verify, without any need of substantiation, if the data concerning himself/herself are (or not) correct and updated. The provision of this information is necessary to satisfy the requirement of fair and lawful processing under the Data Protection Directive and also ensures informational self-determination [2,14].

4 Legal Aspects for Data Storage

The main issue of AAL platform consists on using sensors and profiling techniques that create a large amount of personal information (including health data) flowing the system. However, the health data is considered by European and Portuguese law as "sensitive data", thus requiring reinforced protection. Nevertheless, monitoring and profiling must be done in order to accomplish the minimal requirements for the platform operation, which does not mean that legal aspects are breached. It's important to guarantee the protection of the personal data in the iGenda project, in a way allowing the care-receiver to benefit from the available services and, at the same time, having all warranties of fundamental rights being respected.

4.1 Health data

All AAL platforms must collect health data about their users and store it for historical operations, personal health records and future medical actions based on previous conditions. Therefore, iGenda is confronted with the difficult decision of which categories of personal data, particularly health data, should be collected and stored.

Health data is sensitive data according to Portuguese and European law and its processing may not be authorized in all situations, unless there is an explicit consent of the data subject and additional data security measures are available (article 8º of the Directive and article 15 nr. 3 of the Portuguese Law 67/98). An exception to the requirement of free and informed consent occurs when the care-receiver is temporarily unable to express consent (for instance, because he/she is in coma or totally unconscious) and, yet, the data collection or processing is absolutely essential in order to protect a vital interest of the care-receivers (usually life or death situations) and in this case, the fundamental right to life will always prevail [3]. Another important exception is the treatment of medical data for purposes of preventive medical actions, medical diagnosis, care or management of healthcare services that are carried out by health professional obligated to professional secrecy [2].

The delicate issue of AAL systems and iGenda platform is centered in the establishment of limits to this huge flow of collection, storing and transmission of health data, and these are related with the application of the data protection principles. Since it is crucial to observe fundamental rights of the individual (especially regarding the right to be left alone or the right to be forgotten) so, the data must only be stored while it is absolutely indispensable, assuring a balance between the collected data and the purposes of its collection and processing [2]. The care-receiver must always be informed about the presence of sensors and cameras and what type of personal data is being processed and for what purposes the data is planned to be used, according to article 11º of the Data Protection Directive. Additionally, to guarantee that only personal data that is necessary for each specific purpose is processed, we recommend that AAL platforms should be created with a mechanism of privacy by design and also a privacy impact assessment before it is used.

The Data Protection Directive directly and indirectly affects the process of keeping information about the medical history of the people that are supervised by AAL platforms. In fact, data protection principles represent an important limit to the processing and conservation of personal data under any form, mainly imposing restrictions in the elaboration of automatic profiles based on the personal data treated. To provide a secure and reliable medical diagnosis, it is imperative to have knowledge about previous medical problems. Therefore, by shortening the lifespan of the information, the Directive restricts the provision of any type of diagnosis and just responds to immediate problems.

4.2 Profiling

The essential feature in the iGenda that requires a large amount of personal data is the profiling technique. It automatically creates a database that mirrors the user's personality to better emulate the user's choices in non-critical decisions. In this database, each user is clearly identified and each one has its own profile type, such as care-receiver, the caregiver, and other users.

In accordance with the general rules of Data Protection Directive, when the construction of user's profiles take place, the iGenda (seen in this context as an entity) always informs the care-receiver with the following information: the precise purpose of the collection and processing of his/her personal data (e.g., for diagnosis, prevention), identity and contact details of data consumer, the precise categories of personal data the platform will collect and process, the recipients of the data entitled with the right of access and rectification, ensuring the transparency of all of the process of collection and treatment of personal data and the revelation of information to third parties [8].

These profiles contains various categories of personal data that require different degrees of confidentiality, therefore, each user has different access conditions to the database that includes explicit consent and special technical barriers for data protection.

4.3 Data Access Feature

iGenda features social interaction in highly heterogeneous group of people, connecting several of its users and sharing non-vital information among them. The issue that arises is that there is the possibility of building true knowledge from the crossing of non-vital information. Thus, by propagating previous rules, each individual may require being exempt from this feature and the removal of all information related to him/her. This right is associated to the right to be forgotten and the right to be let alone [2]. The care-receiver should be able to ask about the access of each party and be allowed the possibility of rectification, deletion or blocking of any parties or entities involved in the exchange of information within iGenda. Furthermore, the possibility of sharing personal data is also kept under control of the care-receiver: him/her can deny the collection and processing of his/her personal data and refuse access to optional information using privacy-friendly default options [2], with the downside of losing some or all iGenda features and services.

In the data protection domain, the integrity of the system and the control by the individual on data of his own can be achieved by the use of privacy-enhancing technologies and transparency-enhancing technologies as instruments capable of helping in the fulfilment of the requirements of informational self-determination [8]. The iGenda platform includes regular internal checks and controls of database access, which serve as a protection against intrusions. Therefore, the module of the Agenda Manager keeps a record of every connection made through a logging registry, which registers every communication tunnel established.

Nevertheless, iGenda intensely uses personal data. That is why data security must be implemented directly in the architecture of AAL (privacy by design), from the early design stages. The privacy by design approach has been addressed by the European Commission in their proposal for a General Data Protection Regulation and it can be a solution to some of the legal problems raised by the cross exchange of health data in iGenda, while preserving a high level of data protection. Currently, the iGenda provides some features that followed the privacy by design concept, e.g., encryption of data, login requirements for sensitive data, communication obfuscation, etc.. These are not enough and more is needed to keep the information secure. Moreover, privacy by design has to be carefully considered, as it is relatable to technology and social factors. In terms of iGenda, the privacy by design is considered only applied to the technological features, implementing encryption here possible, assuring digital signatures and enforcing secure database access and communication tunnelling.

5 Technological Implementations

As explained before, iGenda has already some security features implemented. One is the secure access defined by user/password pair. Dealing with mobile devices, there is the possibility of others operating the device unlawfully. The visual interfaces are designed to be simple, and some information is directly displayed but, sensible and private information is protected with identification and passwords. The digital signature assures that the sender of events is the real person. The issue with the iGenda is that currently it does not enforce encryption on the message per se, but the content is stamped with the digital signature. The multi-agent system that sustains the iGenda provides ontologies and encryption to the underlying message system, which for internal messages of the platform is secure enough but not to exchange them over the internet.

Technologically speaking, security measures have their positives and negatives. While the positive are easy to see, the negatives are usually increased complexity and time and resources consumption. While common users may consider that spending a few seconds more in sending a message is acceptable, in a large scale system that time is not trivial nor unnoticeable. For instance, PKI encryption is a proven secure method, but it takes an considerable amount of time to be encoded or decoded (up to a few seconds) that shows an impact when implemented in low computing power systems like sensor platforms [6]. We have considered different approaches, like each user possessing a computer system at home that could decentralize the information but, that would only increase the number of security measures that would have to be implemented. So, the only solution to this issue is to wait for more advanced sensor systems that will have embedded encryption protocols. Until then, we will in the near future implement encryption in the messaging service of the smartphones, reinforcing the strength of the digital signature, but accept non-encrypted messages from other systems.

In terms of database security, the implementation relies on the database provider tools that encrypts in real-time its contents. The issue is the access to the information, and that is considered a social issue. The automatized services do not rely on people to operate and serves the information to the ones who require them. This situation shifts the burden of responsibility to the users. iGenda technicians will be scrutinized and under a non-disclosure confidential contract, which enforces these agents to be private about the information that they edit. Thus, the main issue related to the databases is the time that information is kept.

The profiling methods (and the medical information) require that the information about the users are kept at least during the time he/she is registered in the platform, and in some cases even more. For instance, if a specific user influenced or shared activities with others its information has to stay on the platform even if the user quits the service. It is our belief that other users must not have have reduced services due to others actions, meaning that to keep the actions' history of each user intact, all the participants must be correctly identified. This is a difficult issue to resolve as it goes against two directives, the right to be forgotten and the retention principle. While the retention principle is somewhat easy to be met (as explained before), the right to be forgotten is only partially possible. There are two approaches to achieve it, delete all data related to the user who wishes to opt-out and void the assumption that users should not be impaired by other users actions; or to delete only part of the data and go against the legal ruling. Currently the iGenda is able to partially deleting the information of the users that which to opt-out, eliminating all private information but keeping social information (e.g. name and friends information) and to delete all information available. Although the latter option is not recommended by us.

As interaction occurs there will always be some type of information trail. Therefore, until the Data Protection Directive encompasses new rules about social networks and information sharing it will be impossible to have AAL features fully compliant.

6 Conclusions

This paper presented an AAL project, the iGenda, and its current legal issues. It has analysed the technical features and their legal implications in terms of privacy and data protection. Moreover, it has showed what themes need to be addresses to keep data transmission and data processing within the legal boundaries. The paper also exposes the potential risks of privacy loss and unauthorized access to personal data and what data can be used in accordance with the current data protection framework.

The current legislation greatly limits the use of the iGenda features, even if the care-receiver is allowed to make use of his legal right on informational self-determination by taking control on his own data flowing within the system. The acceptability rates depend on how adequate is the level of data protection and privacy; that is why security-relevant issues must be identified in the preliminary stages of development.

We consider that currently there are only two ways to deploy the iGenda: legally compliant (with subpar features) or not legally compliant (with all features available). Unfortunately, there is no middle ground and if we consider implementations on nursing homes the problem increases exponentially. Nursing homes have to comply with strict legal an ethical legislation that is even more punishing to the iGenda. Considering that the main adopter of AAL services are nursing homes, the development of such technology may be at serious risk.

The main concern is the protection of the care-receiver and its data, in a way that his/her fundamental rights are guaranteed. To achieve this goal, it is critical that new legislation is implemented to better reflect the new AAL technologies and new social structures.

Acknowledgements

This work has been supported by COMPETE: POCI-01-0145-FEDER-007043 and FCT – Fundação para a Ciência e Tecnologia within the Project Scope: UID/CEC/00319/2013. A. Costa thanks the Fundação para a Ciência e Tecnologia (FCT) for the Post-Doc scholarship with the Ref. SFRH/BPD/102696/2014. This work is also partially supported by the MINECO/FEDER TIN2015-65515-C4-1-R.

References

1. Care4Balance: http://www.aal-care4balance.eu/ (2015)
2. Castro, C.S.e.: Direito da Informática - Privacidade e Dados Pessoais. Almedina (2005)
3. Correia, L.B.: Direito da Comunicação Social. No. vol. 1 in Direito da comunicação social, Almedina (2005)
4. Costa, Â., Castillo, J.C., Novais, P., Fernández-Caballero, A., Simoes, R.: Sensor-driven agenda for intelligent home care of the elderly. Expert Systems with Applications 39(15), 12192–12204 (nov 2012), http://dx.doi.org/10.1016/j.eswa.2012.04.058
5. Costa, Â., Novais, P., Corchado, J.M., Neves, J.: Increased performance and better patient attendance in an hospital with the use of smart agendas. Logic Journal of IGPL 20(4), 689–698 (feb 2011), http://dx.doi.org/10.1093/jigpal/jzr021
6. Doukas, C., Maglogiannis, I., Koufi, V., Malamateniou, F., Vassilacopoulos, G.: Enabling data protection through PKI encryption in IoT m-Health devices. In: 2012 IEEE 12th International Conference on Bioinformatics & Bioengineering (BIBE). pp. 25–29. IEEE (nov 2012)
7. Grauel, J., Spellerberg, A.: Attitudes and requirements of elderly people towards assisted living solutions. In: Mühlhäuser, M., Ferscha, A., Aitenbichler, E. (eds.) Constructing Ambient Intelligence. Communications in Computer and Information Science, vol. 11, pp. 197–206. Springer Berlin Heidelberg, Berlin, Heidelberg (2008)
8. Hert, P., Gutwirth, S., Moscibroda, A., Wright, D., González Fuster, G.: Legal safeguards for privacy and data protection in ambient intelligence. Personal and Ubiquitous Computing 13(6), 435–444 (oct 2008)
9. Marques, G., Martins, L.: Direito da Informática. Almedina (2006)
10. Novais, P., Costa, R., Carneiro, D., Neves, J.: Inter-organization cooperation for ambient assisted living. Journal of Ambient Intelligence and Smart Environments 2(2), 179–195 (2010), http://dx.doi.org/10.3233/AIS-2010-0059
11. O'Grady, M.J., Muldoon, C., Dragone, M., Tynan, R., O'Hare, G.M.P.: Towards evolutionary ambient assisted living systems. Journal of Ambient Intelligence and Humanized Computing 1(1), 15–29 (dec 2009)
12. Rashidi, P., Mihailidis, A.: A survey on ambient-assisted living tools for older adults. IEEE Journal of Biomedical and Health Informatics 17(3), 579–590 (may 2013)

13. RelaxedCare: http://www.relaxedcare.eu/en/ (2015)
14. Rouvroy, A., Poullet, Y.: The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In: Gutwirth, S., Poullet, Y., Hert, P., Terwangne, C., Nouwt, S. (eds.) Reinventing Data Protection?, pp. 45–76. Springer Netherlands (2009)
15. Sousa, F., Viola, L., Ferreira, L., Trevisan, G., Cunha, D., Alves, J., Simões, R.: An ecosystem of products and systems for ambient intelligence - the AAL4ALL users perspective. Studies in health technology and informatics 177, 263–71 (jan 2012)
16. Sun, H., Florio, V.D., Gui, N., Blondia, C.: Promises and Challenges of Ambient Assisted Living Systems. In: 2009 Sixth International Conference on Information Technology: New Generations. pp. 1201–1207. IEEE (2009)
17. Tepandi, J., Tšahhirov, I., Vassiljev, S.: Wireless PKI Security and Mobile Voting. Computer 43(6), 54–60 (jun 2010)
18. United Nations: World Population Ageing. No. 4 in 7, UN (2009), http://www.un.org/esa/population/publications/WPA2007/SummaryTables_new.pdf
19. United Nations: Population estimates and projections section. Tech. rep., United Nations (2012), http://esa.un.org/wpp/ppt/paa/PAA_2012_Heilig.pdf
20. Villacorta, J.J., del Val, L., Jimenez, M.I., Izquierdo, A.: Security System Technologies Applied to Ambient Assisted Living. In: Knowledge Management, Information Systems, E-Learning, and Sustainability Research, pp. 389–394. Springer Berlin Heidelberg (2010)