Journal of Ambient Intelligence and Humanized Computing manuscript No.
(will be inserted by the editor)

Security-enhanced Ambient Assisted Living Supporting School Activities during Hospitalisation

**Pablo Antón, Antonio Muñoz, Antonio Maña,
Hristo Koshutanski**

Abstract Children that spend long periods in hospitals suffer different negative effects that affect their emotional and psychological development and their family life. Among these effects, sleep disorders, stress, and degradation of school performance are the most frequent. A common reason behind these effects seems to be related with the disruption of the normal relationships and the lack of contact with the different social groups that the children belong to (family, friends, school, etc.). In this paper we present results of the DESEOS research project, which applies the Ambient Assisting Living (AAL) paradigm to increase the quality of life of health cared children by developing novel devices and applications to enhance the contact with their different daily environments. Security and dependability are central aspects in these scenarios, and consequently are central to the DESEOS solutions. In particular, this paper presents how DESEOS provides a secure solution for one of the project scenarios.

Keywords Ambient Assisted Living · Security · Security Patterns · Children Hospitalisation

1 Introduction

Ambient Intelligence (AmI) is a new concept by which Information Technology is applied to build networks of devices and services that are dynamically connected and collaborate to help people in different activities. These digital environments are aware of the presence of people, and can react and adapt to their necessities, habits, movements, etc. [11]. More precisely, the work presented in this paper focusses on an application of the Ambient Intelligence concept called Ambient Assisted Living (AAL). This technology applies the AmI approach to assist people with disabilities or health problems with the principal aim of allowing them to live independently in their daily life environment. Despite of assist the elderly and disabled [10,4], today more and more

This work is supported by the project **DESEOS** (TIC-4257, **D**ispositivos **E**lectrónicos **S**eguros para la **E**ducación, **O**cio y **S**ocialización meaning "secure electronic devices for education, entertainment and socialization") funded by the government of Andalucía.

Escuela Técnica Superior de Ingeniería Informtica, Universidad de Málaga (Spain)
E-mail: {panton,amunoz,amg,hristo}@lcc.uma.es

scenarios for AAL are being developed. In this paper we consider its application to help children that undergo long-term hospitalisation.

Even considering that the situation has improved over the last few years, children experience that have to spend long periods in hospitals suffer different negative effects that affect their emotional and psychological development and their home life [7][8]. Among the effects that have been studied in relation to the time spent in hospitals we would like to draw attention to :

1. *Sleep disorders.* The experience of the medical and psychological team of DESEOS has revealed that even in cases of mild diseases, the children that stay in hospitals suffer from sleeping disorders that tend to be illnesses, but that can have negative effects on the children' and their relatives' lives.
2. *Stress.* Stress is one of the most common effects of a stay in hospital, both in children and their parents [2]. Studies reveal that this stress is caused to a great extent by the situation of isolation and lack of contact with their daily environments.
3. *Consequences on school performance.* No doubt that any sickness has a negative influence on a child's education [9]. This is heavily influenced by the lack of human contact and affection [1]. The studies show that this happens even in cases where the disease or sickness did not have a direct influence on the capability and abilities of the child to study.

A common reason behind all these effects seems to be related to breaking off of the normal relationships and the lack of contact with familiar environments (family, friends, school, etc.).

A large number of security issues appear in these heterogeneous and dynamic systems [17], such as:

- User unawareness of the AAL devices in the environment increases the risk of compromising user privacy and confidentiality.
- Devices unawareness of context changes and dynamic interactions with other AAL devices increases the risk of security and privacy violation of data exchange.
- How to guarantee access control on user data being processed by different AAL devices interacting with each other.

1.1 Paper Contribution

The main target of the DESEOS research project is the development and application of secure AmI technologies for AAL systems to increase the quality of life of children in health care. DESEOS was designed with the aim of helping to improve the aforementioned problems by developing novel devices and applications to enhance contact with the different daily environments of the child. This goal is achieved based on functional developments, but it also entails risks that must be addressed from a non-functional point of view, in particular those related to security, privacy and dependability. To address the security requirements we take advantage of the SERENITY approach [16], which is a framework based on the concept of "Security and Dependability Patterns" (S&D Patterns) [3]. S&D Patterns are an evolution of the classic Security Pattern defined by Schumacher [13].

The main goals of the SERENITY project were the definition of a security-aware engineering process for developing systems that require dynamic adaptation at runtime, supported by rigorous engineering practices and realized by means of a set of tools

spanning the full system life-cycle. As such, all concepts of security patterns and classes have been realized as generic software solutions in SERENITY. However, an issue that was out of the scope of SERENITY was the application of these concepts in domain-specific scenarios and therefore a future challenge which has been identified is how to provide appropriate security and dependability mechanisms in different areas of ICT based on the SERENITY framework.

The DESEOS project makes a step beyond SERENITY by adopting SERENITY results to provide security and dependability solutions to a real-life AAL scenario using cameras, TV screens, and other devices with technologies,security requirements and solutions that are specific to this domain.

The rest of the paper is structured as follows. Section 2 presents the DESEOS AAL scenario with the various types of AAL devices adopted, and the security requirements inherent in the scenario that the paper contributes to. Section 3 presents an overview of the SERENITY project approach underpinning the DESEOS security model. Section 4 discusses the DESEOS security architecture and its corresponding message flow. Section 5 presents DESEOS security requirements and approach to enable secure and trusted communications. It also discusses adopted security protocols, components and solutions. Section 6 presents the DESEOS security solution and design of S&D artefacts underpinning DESEOS secure communication. Section 7 oulines the related research projects in the field of AAL. Section 8 concludes the paper and presents future work.

2 DESEOS AAL Scenario

The main objective of DESEOS is to build an AAL environment to improve the quality of life of hospitalised children, both during the hospitalisation period and during post-hospitalisation. In order to achieve this objective the research and development in DESEOS is guided by several selected scenarios. In this section we present one of these scenarios in order to illustrate the kind of situations and systems that DESEOS deals with. The scenario focuses on providing a means to reduce the problems caused by long-term hospitalisation of children and involves two spaces (physical environments): Hospitals where children are hospitalised; and Schools where the hospitalised children's classmates and teachers are. Within the scenario we consider several roles depending on the actors that interact such as pupils, parents, teachers and doctors, and the space where the activity takes place mainly a hospital and a classroom, but also we consider children's home (in case post-hospitalisation requires staying at home).

The general aim of the presented scenario is to allow the hospitalised child to continue attending school in his own class. Although all hospitals have a school where children can continue their education, we believe that the most important aspect that the child loses is not just the education (lectures, tuition and exercises) but the human contact and the integration in the group (class).

Several secondary aims guided us whilst building the DESEOS scenario:

- *Visual contact*. Eyesight is one of the main elements used in human communication and interaction. Providing technical means for maintaining visual contact in the most natural way so that the child feels that he is attending his habitual class is therefore very important. For this purpose, we provide a special type of video streaming service that we call "virtual window" because it acts like a window' changing the part of the classroom displayed depending on the position and viewing angle of the hospitalised child.

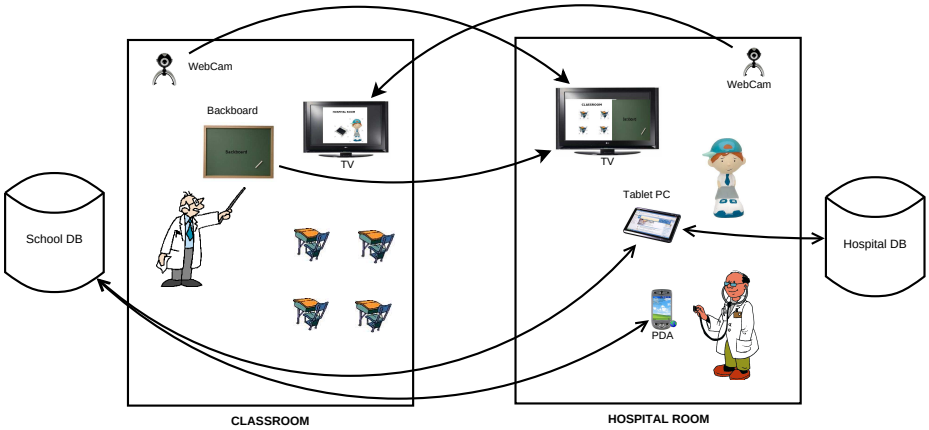

Fig. 1 DESEOS Application Scenario

- *Auditory contact*. Another essential aspect of communication is auditory contact. It complements the visual contact helping the child to fit in his classroom as any other classmate. This is achieved by positioning different microphones that are mixed depending on the relative position of the child and the virtual window.
- *Medical and school information access*. In every situation there is certain information related to the hospitalised child that is used by different actors. The level of access and the specific information that is made accessible is determined dynamically depending on the situation, the context and the actor.

We consider the following elements in each space:

- A set of devices which form a local AAL environment: TV screens, webcams, microphones, electronic backboards, PDAs, and Tablet PC.
- Information systems of a particular realm: servers, databases and a corresponding network connection.
- A set of people who play different roles: teachers, pupils and doctors.

Figure 1 illustrates the elements in each of the spaces of the scenario. These elements are used to fulfil the aforementioned goals. For instance, movable webcams and TV screens are used for achieving an ideal level of visual contact by implementing a virtual window application and the replication of the classroom blackboard in the hospital room. To increase the feeling of natural interaction we use an accurate positioning system for the viewer (the hospitalised child) so that we can simulate the sensation of looking through a window by using camera movement, zooming and pan. The positioning system uses a bluetooth infrared camera. For economic reasons we use a Nintendo Wii® console remote for this [6].

We note that the scenario of the hospital realm can also feasibly be applied to pupils' home settings ,once discharged, during the recovery period. The devices defined in the scenario are quite common that can be found in more and more houses nowadays.

Another example of information sharing among the two spaces is when a doctor enters the hospital room and uses his PDA to access information provided by the school via the DESEOS system in order to provide tutoring and/or monitoring of the pupil.

We classify AAL devices as the following types based on their functionality and processing capabilities:

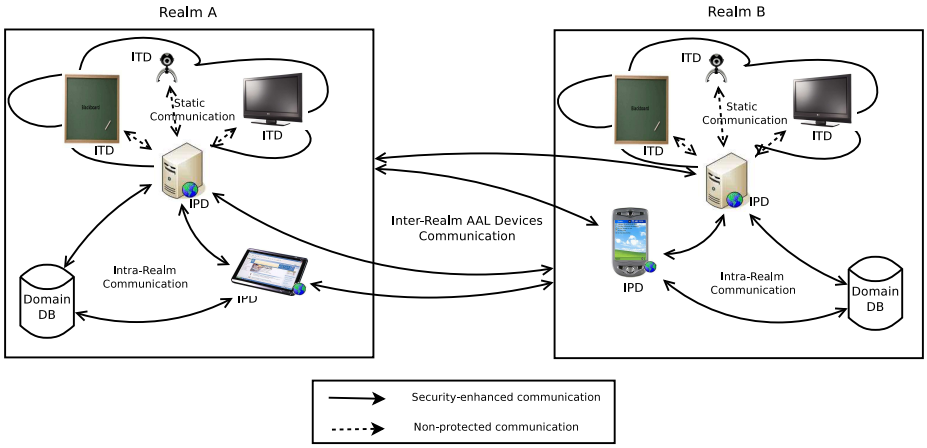

Fig. 2 DESEOS AAL Devices Communication

- *Information Transmission Devices (ITD)* are specific types of devices that have the capability of capturing about their environment information and transmitting it to an external device for further (digital) processing. These devices (webcams, microphones and electronic blackboards undertake the role of transmitting information. We note that TV screens could also be seen as a type of ITD device. However, we consider them as computer peripheral devices that visualize computer-related information.
- *Information Processing Devices (IPD)* are those types of devices that provide the capability of processing digital information and making it available to computer-related operations or communications (desktop computers, laptops or tablet PCs are examples of this category). Often, ITD devices are statically connected to IPD devices for real-time processing of environment information. The IPD devices have dedicated computational capabilities of managing and collaborating with other ITD devices as well as running DESEOS applications.
  There are IPD devices that also play the role of ITD devices (PDAs, Tablet PC and smart phones are in this category), where environment information is captured and processed on the same device. In this case, we classify those devices as IPD (and not as ITD).

A key application of the DESEOS scenario is the *VirtualWindow* application. It displays class activities in school, and assigned homework, moreover it shows pupil activity in a hospital on the side of the school realm (as shown in Figure 1). The VirtualWindow is a DESEOS application that runs on the computer, specifically on the IPD device, to which the webcam and the microphone in the hospital room are connected. As we mentioned, DESEOS applications are installed into IPD devices, as well as all security-related aspects.

Figure 2 illustrates DESEOS device communication and shows whether communications are protected or not. The figure shows that all ITD-type devices communicate with other ITD devices via the corresponding IPD device that they connected to. In other words, to be part of the DESEOS network an ITD device has to be connected to a IPD running DESEOS applications. In that way, all inter-realms, as well as, intra-realm communications occur via IPD-type devices. For example, to show school activ-

ities captured by the ITD devices in a classroom, the VirtualWindow in the hospital realm connects to the IPD device that is processing classroom activities and visualizes those on the TV screen in the hospital room.

However, all devices shown in the diagram have a role to play in order to facilitate the interaction and contact between hospitalised children and their schools from a functional point of view. Several security problems arise due to the nature of the information being handled (medical, scholar, video, etc) that impose challenging security requirements to the previous elements. To address the security problems we need to extend the SERENITY model, which improves the scalability and allows an easy and secure integration of new devices in the system.

2.1 Security Requirements of the Scenario

The described above scenario entails several security requirements which are the basis for building core security solutions presented in Section 6.

- *Confidentiality and privacy* of communications (of audio, video, text, emails etc) refers to data confidentiality when transmitted across local and/or Internet network. For example, if a pupil is an epileptic child or that a particular pupil must take a medicine during class time, the teacher must be informed, so, the privacy and confidentiality of medical information is identified as a requirement in this case. When a pupil sends his or her homework to the school system (during his stay in hospital) confidentiality of his homework data is identified when transmitted to the school system.
- *Role/attribute-based access control* to school-related resources accessed by teachers, pupils, doctors, and so on. Different conceptual roles must be handled by implementing a proper role-based access control model. As part of the access control requirement is delegation mechanisms, for example, post-hospitalisation a school can delegate the right of a doctor in the hospital to access pupil's data in school where teachers store observations on the pupil's health (e.g. when following a specific).
- *Non-repudiation* on certain actions/events done. For example, during the recovery process teachers can monitor if the child is following the doctor's instructions whilst attending school activities and prescription make note of their observations in a school database especially designed for this purpose. Another use is when pupils submit their homework (during their stay in hospital) and non-repudiation on these actions is required.
- *Authentication* of network entities such as school information servers, authentication of pupils when given access to the school database, authentication of doctors when accessing teachers observations on pupils' health, etc.
- *Accountability* of those who accessed certain data of the school information system such as teachers, pupils, doctors and so on. This requirement is closely related with authentication and confidentiality requirements.

3 SERENITY Project Overview

As we will see in Section 7 the AAL paradigm has reached a level of research and development that calls for the need of scalable and tailored security solutions well-aligned

with the number of AAL-related application models. In this context, the SERENITY project produced novel models and life-cycles of secure systems that are able to evolve dynamically to adapt to the changes in their operating context.

It is important to clarify that we cannot consider any pure AmI scenario for the time being, since AmI is an emerging concept and current technologies do not allow fully-fledged AmI deployments in the widest sense of the term. However, the proposed scenario shows the key characteristics of AmI environments. In particular, the scenario shows that in addition to the impact in the future AmI scenarios, the SERENITY approach can have a short-to-medium term impact as an enhancement of many current technologies.

SERENITY [16] addresses security and dependability in the complex world of Ambient Intelligence by providing an infrastructure for the development and application of adaptable S&D solutions in dynamic and continuously changing AmI ecosystems. It also provides concepts, methods, processes, and tools that underpin this infrastructure and supports S&D experts, S&D engineers, application developers and system administrators in their tasks.

SERENITY is based on two main cornerstones [14]: on the one side capturing the specific expertise of security engineers in a way that permits its automated processing; and on the other side providing a means to control systems during runtime by performing run-time monitoring of security and dependability mechanisms. These have materialized by means of three innovations:

1. A set of modelling artefacts, called S&D artefacts, used to represent security and dependability solutions (S&D Solutions) at different levels of abstraction. S&D Solutions are monolithic components that provide security and/or dependability services to applications. The use of different levels of abstraction responds to the needs of different phases of the software development process. These artefacts are supported by an infrastructure for the development and the validation of S&D Solutions. This infrastructure includes concepts, processes and tools used by security experts for the creation of new S&D Solutions.
2. The SERENITY Development time Framework (SDF) enables developers to choose the best solutions to fit the requirements of their applications. Security experts use these on-line repositories of S&D artefacts (called SDF S&D Libraries) in order to publish the S&D solutions they develop and to make them available to clients. Application developers access S&D Libraries when they are developing SERENITY-aware applications in order to look for the S&D solutions that are needed for fulfilling their requirements. A detailed description of the development of application based on these on-line repositories can be found in [15].
3. A runtime infrastructure, called SERENITY Run-time Framework (SRF). SRF provides support to applications at run-time, by managing S&D Solutions and monitoring the systems context. SERENITY-aware applications are developed with open architectures that are completed at run-time by the SRF. SRF is the tool that enables the dynamic configuration, binding, monitoring and replacement of S&D mechanisms within applications, thus achieving the core of the SERENITY approach. The SRF is implemented as a service running in a device, on top of the operating system, and listening to applications' requests. Applications send requests to SRF in order to fulfil their security requirements. The SRF translates these requests into S&D Solutions that may be used by the application. As a result of the selection process, the SRF instantiates S&D Patterns or Integration

Schemes by means of Executable Components and makes them accessible to the applications. External systems interacting with an instance of the SRF will be able to monitor that the behavior of the framework and the executable components running in it is correct. With these interfaces, the SRF provides support for the dynamic supervision and adaptation of the system's security solutions to react to the changes in AmI ecosystems.

SERENITY provides four main S&D artefacts to represent S&D solutions: *S&D Classes*, *S&D Patterns*, *Integration Schemes* and *S&D Implementations*. These S&D artefacts, depicted in figure 3, represent S&D solutions using semantic descriptions at different levels of abstraction. In the figure the actual components are referred to as Executable Components.

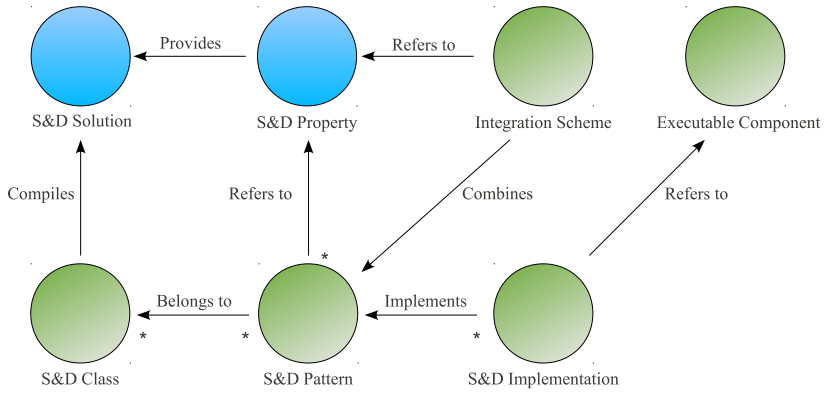

Fig. 3 SERENITY Artefacts Model and Component Relations

The benefits of the SERENITY approach have been demonstrated through prototype systems that use the artefacts and infrastructure of SERENITY to solve real S&D problems. Overall, SERENITY has already made significant contributions related to the dynamic configuration, deployment, monitoring and adaptation of security and dependability solutions in AmI ecosystems, opening new paths of possibilities and some challenges.

4 DESEOS Security Architecture

DESEOS security architecture is divided into two functional elements: client-side security and server-side security components. Figure 4 shows high-level security communications between DESEOS components. The DESEOS SRF is an evolution of the SERENITY SRF and is the core component installed in devices that has to communicate with the school information system. It is important to highlight that DESEOS SRF is installed either in the device itself (if feasible, such as PDAs, or tablet pc) or in the accompanying computer part that is connected to the device (such as in the computer that a TV screen and/or a webcam are connected to).

Figure 4 shows both the DESEOS SRF and the application communication. It shows that DESEOS SRF handles all security aspects of AAL device communications

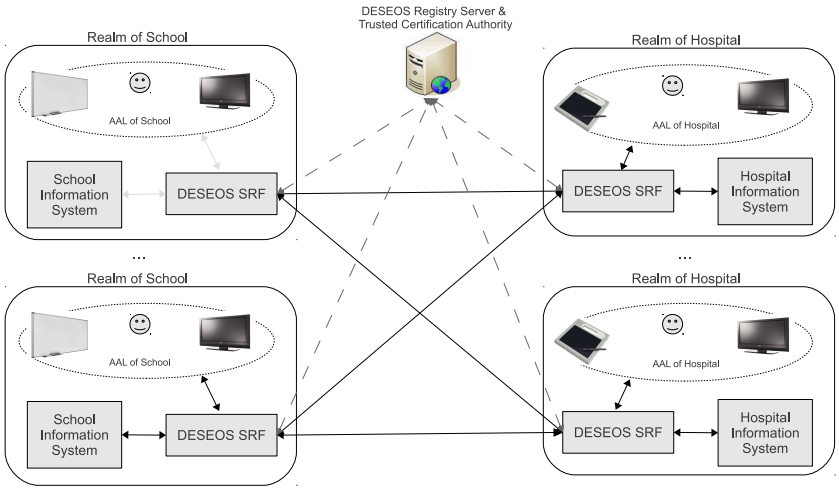

Fig. 4 DESEOS Security Communications Conceptual View

between realms. The figure also shows that the hospital information system can use their DESEOS SRF when hospital personnel need to access the school system, for example when doctors have to monitor pupils health during school activities as reported by the teachers in the school.

On the school domain, the DESEOS SRF is used (i) to interface security aspects when local AAL devices interact with the school information system for storing data for subsequent use by hospital (remote) AAL devices, and (ii) to interface security aspects of the school information system when establishing communications with remote AAL devices of a hospital. The former case is considered when the school wants to avoid someone in the school local area network learning what data is exchanged between the school AAL devices and the school information system. The latter case is considered to free school security administrators of taking decisions about which specific security solutions are appropriate to be used for the school system. Often this knowledge is beyond the scope of system administrators and this is the case where the SERENITY approach contributes massively.

The link between local domain AAL devices and the local information system is not necessarily secured for all communications. Only when the local domain policy postulates the need of confidentiality and privacy requirements for those communications the SRF is used to provide the best solution to fulfil those requirements. However, all communications between hospital's AAL devices and the school information system have to be secured and access controlled.

The DESEOS architecture aims at addressing several schools and hospital domains where pupils are during their stay in a hospital, with DESEOS system installed, to allow the full participation in classroom activities and lessons of the corresponding school. To enable this, DESEOS network consists of a registry server and several DESEOS SRFs correctly configured to enable trusted relationships with the DESEOS network.

The registry server has two main functional roles: serving as a trusted certificate authority to all DESEOS SRF communications, and serving as "DNS"-like school domain resolution. For example, when a school wants to install a DESEOS system to enable its pupils to access school activities when staying at any hospital where DESEOS is

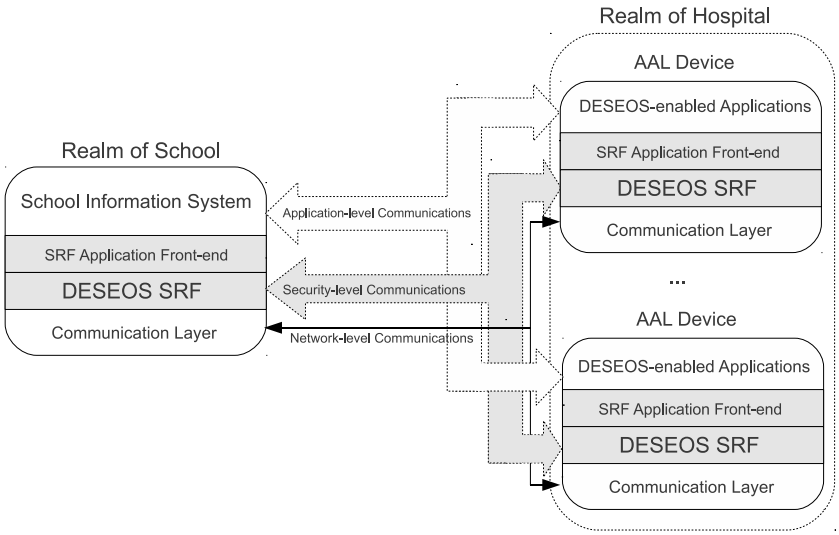

Fig. 5 DESEOS Security Architecture and Communications

installed, the school has to be registered in the DESEOS registry server including the specific domain and network information of service access to that school's information system. The outcome of the school registration is school certification by the DESEOS trusted certificate authority indicating the school is a recognized one within the DESEOS network of schools. This certificate information is installed in the school's DESEOS SRF module that, in turn, uses it to establish trusted communications with other registered SRFs in hospitals and schools.

The DESEOS SRF, on the side of a hospital AAL domain, is used to interface security aspects of applications communicating with potentially different schools depending on current pupil's school membership. For that purpose, each school registers a pupil to the DESEOS registry server to obtain a digital certificate certifying pupil's name, school membership, internal school number and so on. The outcome of the pupil registration is a certificate that is installed in the DESEOS SRF of the AAL devices in the hospital where the pupil is being cared for.

When the pupil is staying in the hospital and is to join in classroom activities the most important security aspect is to enable secure communications with the corresponding school information system. To do so, during the set up phase, the DESEOS SRF at the AAL device uses the locally installed pupil's certificate to obtain their school's name, and connects to the DESEOS registry server to obtain technical information on network end-point address of the school information system and available APIs used for that school activities. In that way, the DESEOS applications are already configured to interact with the school system and visualize school activities.

Figure 5 shows the DESEOS SRF-level security communications with respect to the application-level communications. An important part of the DESEOS SRF is the accompanying SRF front-end component. This component fulfills the role of *security abstraction* layer between DESEOS-enabled applications and DESEOS SRF. The DESEOS SRF application front-end can be seen as a set of plug-ins to the DESEOS SRF that depending on what type of applications need to ensure security properties

the respective plug-in is will be used. For example, all types of applications that use multimedia streaming protocols to display classroom activities will need a predefined application front-end for enabling those applications to use DESEOS SRF. Part of DESEOS project contribution is to provide an initial set of application front-ends for the applications of the DESEOS application scenario.

Each DESEOS SRF comes with pre-installed and pre-defined security patterns, their corresponding security solutions and a security policy. Part of the security policy is provided in the form of a template that is *automatically* instantiated when a given pupil's or school's certificate information is locally installed. The automatic policy instantiation takes place during the set up phase of a DESEOS SRF component and ensures that system administrators are not required to manually intervene in those settings as this is an error prone process. We note that DESEOS SRFs of schools and of hospitals have different security policy configurations but have compatible security patterns and solutions installed. More precisely, the DESEOS SRFs of hospitals may have different patterns and solutions configured with respect to each other because some AAL devices may have limitations on possible security solutions used while others allow a wider range of solutions. On the other hand, DESEOS SRFs of schools have a super set of security patterns and solutions with respect to all possible DESEOS SRFs in hospitals, thus achieving support and compatibility with all DESEOS SRFs used in hospitals.

4.1 DESEOS Certification Aspects

We have decided that different actors of the DESEOS network are to be registered in order to use security solutions provided by DESEOS SRF when interacting with remote hospital or school realms. There is a DESEOS certification authority that certifies different entities in the DESEOS scenario, and this is an important aspect to enable decentralised trust establishment of hospital-school communications. The DESEOS registry server provides all registry-related services.

However, the DESEOS SRF components of the DESEOS network are not intended to be certificate authorities issuing certificates to entities in contrast to a certificate authority network. The goal, and main contribution, of DESEOS SRF is to provide all necessary solutions, in a proper run-time software framework, enabling all DESEOS AAL devices to establish secure and trusted communications between hospital and school realms.

4.2 DESEOS Main Security Assumption

DESEOS SRF relies on the presence of a trusted underlying platform (operating system) for correct execution of its security components. This assumption is often fulfilled by the fact that AAL devices are connected to dedicated computers which have no public access by external entities (e.g. in the case of hospitals), or are used for other dedicated tasks requiring trustworthy OS (such as school information system servers). We note that a possible approach to mitigate the above assumption is to run DESEOS SRF onto TPM-equipped platforms [19], which is part of our future work.

5 Enabling Secure Hospital-to-School Communication

We say that an AAL application is a DESEOS-enabled application when it is designed to interact with the DESEOS SRF (by an appropriate DESEOS SRF front-end). A main goal of DESEOS security architecture is to dynamically provide, in a transparent way, appropriate security solutions to applications of the DESEOS AAL scenario.

However, it is important to note that by just providing security solutions to DESEOS-enabled application is not adequate as it still leaves the application developer with the burden of understanding what a security requirement means in a given context and if that security requirement is exactly what a developer needs for a given application. For example, even providing security patterns for privacy, confidentiality, authentication and access control it is not enough because they may still be difficult to be used in combination by an average application developer (unless the developer has a good background in security). For that reason, we decided to go further and provide a higher level of security properties and solutions by using integration schemes, which simplify the inclusion of complex security mechanisms combining several solutions.

Additionally, we have analyzed, in the context of possible DESEOS application scenarios, what the most frequent requirements for DESEOS-enabled applications are in terms of security, and have captured those solutions as security patterns. We have identified that the applications in the context of DESEOS mainly need to establish secure communications with the school system and access different data about children.

We designed a security solution to be used by all DESEOS-enabled applications when interacting with the school information system without creating the necessity for an application developer to have any specific knowledge of underlying security properties and definitions. To enable the above simplified security solution we also have to look at the school side and what security requirements the school defines on all DESEOS-enabled applications in hospitals.

We will present the integration scheme of the DESEOS SRF where we define secure and trusted communications between DESEOS-enabled applications and a school information system.

We have devised a scheme that is generic enough to also be used for non-hospital realms, such as from children's houses, especially for children stay at home during convalescence.

We will use two DESEOS applications (the most relevant to the first pilot case of the DESEOS project) to illustrate the security aspects underlying secure communications of those applications with a school system. A screen in a hospital is connected to a local computer that runs both applications simultaneously but visualizes the results of the two applications in different parts of the screen. Usually the screen is divided in two smaller screens each showing the interface that interacts with the child.

First application visualizes real time activities in the classroom. There are cameras in the classrooms that if active transmit video of the activities in the room, for example teachers. This application shows all audio and video aspects of the classroom.

The second application shows the pupil's related database information retrieved from a school database regarding their activities, such as homework, marks, evaluation of exams etc. This application also allows the pupil to write his homework and remotely send it to the school so that the teacher can check it at their convenience.

First application uses specific APIs of the school system to which it connects to gain access to audio and video streaming of a classroom conforming to given protocols,

while the second application uses WS APIs defined by the school information system to access its database records.

Both applications require authentication of the child in order to assign them the correct classroom streaming data, as well as, to retrieving the database information relevant to the pupil. For this reason the DESEOS security system assigns to each pupil on being admitted, an identity certificate that identifies the kid's name, school ID, pupil's internal school number and so on. Note that in addition to the child's name, the school may include more identifying information where it is relevant. On the other side, DESEOS system assigns to the school information system a certificate that identifies the school system by its domain name, school ID, organization administrating the school and so on.

The pupil identity certificate is installed locally during configuration of the DESEOS SRF modules of both applications described above. The school policy postulates that all DESEOS applications in a hospital have to use secure and trusted communications with the school information system, in order to guarantee privacy and confidentiality of pupil activities within the school.

It is important to highlight the high-level security requirement that DESEOS security system has to provide an application-independent way. This means that without tying a security solution to any of the applications above the DESEOS SRF has to ensure that any of the applications now or in the future can seamlessly use the DESEOS security modules without the additional cost of re-design and re-implementation of the DESEOS security system.

DESEOS SRF integrates the following solutions represented as S&D Patterns and ISs for ease of use and dynamic control.

- Access control solution based on iAccess[1] system and its underlying model [5].
- Web services solution for confidentiality and integrity of SOAP-based WS APIs communications based on Metro[2] high-performance web services security stack.
- TLS[3] protocol implementations of confidentiality and integrity of internet communications and multimedia exchange:
  - Metro security implementation of TLS/SSL.
  - OpenSSL[4] implementation for TLS/SSL.
- Digital certificates (credentials) support of X.509 v3 standard [20] implemented based on bouncycastle[5] cryptographic solutions.

The access control system iAccess provides an interactive access control solution where a server interacts with a client agent asking for the necessary credentials to allow access to a service. The access control solution is suitable in the context of DESEOS project where different applications run on behalf of users and different access control requirements can be automatically negotiated between a user and a server.

The access control system requires a secure and confidential channel – either over a SOAP-based communications or over SSL-based protocol, for example HTTPS – for bilateral establishment of access rights. Currently, iAccess integrates over Metro web services solution. On its side, Metro establishes a secure and confidential channel

[1] `http://www.interactiveaccess.org`
[2] `https://metro.dev.java.net`
[3] `http://tools.ietf.org/html/rfc5246`
[4] `http://www.openssl.org`
[5] `http://www.bouncycastle.org`

between a user and a server by using either WS-Security standard or SSL protocol depending on the application-level context information.

Digital certificates are well suited for decentralized authentication and access control. In DESEOS we adopted X.509 v3 certificate standard due to its wide commercial and non-commercial usage. DESEOS SRF provides implementation of X.509 v3 certificates based on bouncycastle cryptographic solutions. We note that Java and .Net natively support X.509 certificates but only identity (public-key) certificates, which is not a complete solution for the needs of DESEOS where we also need to attribute certificates for expressing users' access rights.

Another important usage of digital certificates (beyond authentication and access control) is the ability of digitally signing documents and other electronic files. Metro security solution provides well-defined Java-based APIs for digital signatures on XML documents as well as on other file formats, while the openSSL provides an equivalent digital signature solution for non-java based applications. This aspect allows DESEOS SRF to provide a solution for non-repudiation requirement, as discussed earlier. It is important to note that the secure communication scheme of DESEOS provides, in an implicit way, non-repudiation of all message exchanged between pupil's applications and school information systems. This is achieved by proper monitoring and logging of all messages exchanged on both DESEOS SRFs at the device and in the school system.

The DESEOS SRF automatically, from the context, applies for audio and video streaming data protocols the TLS protocol implementation to achieve secure and confidential channel between the pupil's application and the school information system. TLS is used when controlling multimedia communication sessions such as voice and video calls over IP, for example, SIP[6] over TLS, or XMPP[7] over TLS, or RTSP[8] over TLS.

In this scenario, we use TLS protocol to enable user-side certificate-based authentication for lightweight user authorization to correct school and classroom activities for the case of audio and video streaming services.

Since TLS protocol provides basic solutions for confidentiality and integrity used by both applications and other security solutions such as access control, we were led to provide at least two underlying implementations of TLS: (i) Metro implementation of TLS - used mainly when access control system is selected to be used by the DESEOS SRF, and (ii) openSSL implementation when DESEOS SRF needs lightweight (memory size restricted) confidentiality and integrity solutions, or providing confidentiality and integrity solutions for non-java based application integration.

The current DESEOS security system integrates Java solutions, but solutions developed with other programming languages can also be accessed thanks to the standard interface provided by the SRF. In fact, the SRF facilitates the integration of these solutions.

5.1 Integration with Legacy Applications

Another important aspect of DESEOS potential adoption is its policy on potential integration with legacy applications and tools. A hospital information system may

[6] http://tools.ietf.org/html/rfc3261
[7] http://tools.ietf.org/html/rfc3920
[8] http://tools.ietf.org/html/rfc2326

have legacy requirements on third-party applications running in the hospital realm. For example, an important aspect of the policy is defining a means by which DESEOS SRF behavior can be monitored externally by legacy applications.

There will be dedicated monitoring-related API allowing legacy applications to request a logging "pipe" of DESEOS SRF to an external destination where all DESEOS SRF behavior is externally logged and monitored. There will be dedicated configuration settings where legacy applications select granularity and type of messages DESEOS SRF outputs to the external destination, such as, what security solutions are being used, what type of communications are secured, what messages are exchanged, what AAL devices are connected, what pupil identity is, what school domain name is, and so on.

On the other hand, if (legacy) applications want to use DESEOS SRF in order to access a school information system, there is a requirement that applications have to provide necessary monitoring aspects to DESEOS SRF, so that DESEOS SRF can ensure proper logging and monitoring of those applications when providing security solutions.

6 DESEOS Security and Dependability Artefacts

We denote with a prefix "`C_`" a definition of a class of related security solutions corresponding to a SERENITY Class artefact. Similarly, we denote with prefixes "`P_`", "`IS_`" and "`I_`" the representations of respectively descriptions a simple or atomic solution corresponding to a SERENITY Pattern artefact, an combined solution name corresponding to a SERENITY IntegrationScheme, and an implementation corresponding to a SERENITY Implementation artefact.

We said in Section 5 that application developers should not be forced to have specific knowledge of underlying security properties in order to enable secure school communication. For that reason, we have designed a special abstract class, called C_SecureCommunication that aims at providing the highest possible abstraction of security to facilitate easy and smooth integration with DESEOS-enabled applications. We have then defined the following two fulfilments of the abstract class by means of Integration Schemes:

- `IS_SchoolSecureCommunication` applying the security solution, described in the previous section, that enables secure and trusted communications with a school information system,
- `IS_HospitalSecureCommunication` carrying out a security solution to enable secure and trusted communications with a hospital information system.

The corresponding implementations of both IS above are I_SchoolSecureCommunication and I_HospitalSecureCommunication.

In other words, at design time, each DESEOS application should adopt the property secure communication, described by C_SecureCommunication, for all external interactions (any message exchange) to an application and its AAL device domain information systems. This is the case of the VirtualWindow application described in Section 2. In the moment of development, a developer should secure all communications of a DESEOS-enabled application by using either IS_SchoolSecureCommunication when the application interacts with a school information system, or IS_HospitalSecureCommunication when the application interacts with a hospital information system.

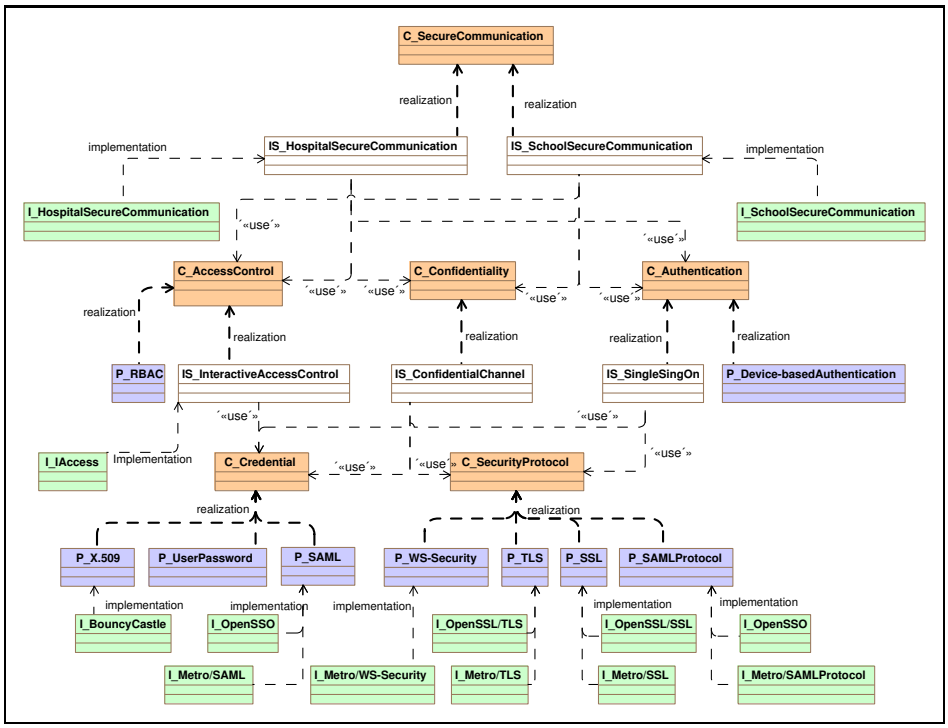

Fig. 6 DESEOS S&D Artefact Structure Enabling Secure Communication

There is a run time security integration process implemented by I_SchoolSecureCommunication and I_HospitalSecureCommunication, which ensures secure and trusted communications with remote information systems.

Figure 6 shows the DESEOS S&D artefact structure enabling secure communications between school and hospital realms.

All communications of the DESEOS scenario in Section 2 are based on predefined services with corresponding APIs at the school information system providing corresponding access to the school database, video and voice streaming of class activities, and so on. Given that, we have found that the most intuitive and transparent way to allow DESEOS-enabled applications to benefit from the developed S&D solutions is to provide all APIs of the school (related to the DESEOS application scenario) accessibility via the IS_SchoolSecureCommunication. Similarly, all APIs of the hospital information system (those related to the DESEOS application scenario) are provided by IS_HospitalSecureCommunication.

In that way, from an application developer's point of view, each of the above IS provides a set of locally accessible APIs signatures[9] of their corresponding remote APIs, so that the developer should access the APIs replicas instead of directly accessing the remote APIs. In turn, the implementation of the IS provides the actual security and trust aspects of all communications to the remote APIs in a way, transparent to application developers way.

[9] The interface part of the APIs only, not their functional body.

For example, all APIs of the school information system related to the DESEOS scenario are replicated as locally accessible via the IS_SchoolSecureCommunication, so that an application developer has to use the locally provided APIs, as he was interacting with the remote school system, but accessed via the IS_SchoolSecureCommunication. In turn, the implementation of IS_SchoolSecureCommunication dynamically integrates all security properties necessary to access the APIs, and invokes the equivalent remote APIs over a security-enhanced communication channel. From an application point of view, the IS_SchoolSecureCommunication plays the role of a "transport layer proxy" that forwards inputs of APIs from local replicas to remote APIs and outputs of those APIs back to the application that invoked the local replicas APIs.

We have the following *run-time* security integration process (steps) upon accessing an API of IS_SchoolSecureCommunication by an application:

1. Establish a confidential channel between the application and the remote school system by using confidentiality property realization, named IS_ConfidentialChannel. Establishing a confidential channel integrates a security protocol and credentials enabling remote system authentication. The remote system, in turn, requires user-side authentication by means of user credentials. The underlying security protocol fulfilment is configured to the user's certificate given by the school and signed by a trusted DESEOS certificate authority (cf. Section 4).
   The IS_SchoolSecureCommunication decides what security protocol is appropriate to use for confidential channel establishment depending on the nature of the API. For example, if video streaming API is being invoked then TLS is the preferred protocol fulfilment, or if WS API access to school database is required then WS-Security protocol is used. We note that all APIs provided by the IS_SchoolSecure-Communication have predefined media network communication by the school information system, and, as such, it is easy to encode that information on the level of the IS's implementation.
2. Once a confidential channel is established, the next security integration step is of access control. We have integrated the iAccess system, an implementation (I_IAccess) of the defined S&D Pattern of interactive access control (IS_InteractiveAccessControl). IS_InteractiveAccessControl defines an automated access rights establishment mechanism between an application and a school information system and uses credentials for attesting user's rights. More technically, the I_IAccess requests the remote API at the school system and awaits if the need of more access rights are requested by the corresponding school IS_SchoolSecureCommunication implementation. Then, an interactive process is triggered between the user device and the school system for granting access to the API.
   The IS_SchoolSecureCommunication integrates all interactions of I_IAccess over the confidential channel established in step 1.
3. If access is granted, the IS_SchoolSecureCommunication performs (again) the remote API invocation with the already established access rights and over the confidential channel of step 1, and returns back the outcome of the API to the application level. From then on, all subsequent interactions by applications (run by the pupil) with access to the APIs of the school system will use the already established security channel and associated access rights.

Since user authentication is performed as part of IS_ConfidentialChannel and its underlying security protocol (client-and-server mutual certificate authentication) there is no explicit user authentication pattern. However, in case where several schools fed-

erate to enable unified access to their services, we have defined the need of explicit Single Sign-on (SSO) pattern as an integration scheme IS_SingleSignOn that uses P_SAMLProtocol fulfilment of the class C_SecurityProtocol to enable an SSO mechanism, and the use of C_Credential as a means of authenticating users. The SSO fulfilment is an ongoing work based on the open source implementation of openSSO.

By the time being, DESEOS SRF implements X.509 standard for the fulfilment of credentials attesting users' identities and attributes. We have used the security policy specification of the iAccess system for attribute-based access control model specification. We use attribute certificates to describe users' group/role assignment, such as user, teacher, visiting doctor, etc.

However, in the case of IS_HospitalSecureCommunication for enabling secure communications with a hospital information system, we identify a real need of an RBAC model, as most of the hospital information systems base their access control on roles and related role hierarchies. We have also identified the need to provide device-based authentication in cases when access to certain hospital services/resources has device-aware control. For example, when a DESEOS AAL device (such as a tablet PC or a PDA) has to access some pupil's data in the hospital information system, the hospital policy may require, in addition to user authentication, a device owner authentication (device-based authentication) in order to ensure better control of hospital data release. We note that access to hospital data a stricter form of control than access to school data due to several privacy aspects. The work on IS_HospitalSecureCommunication is ongoing.

6.1 Security Engineering Approach

We find that it is important to clarify DESEOS approach towards security engineering. We define security requirements for the DESEOS scenario as a means by which we provide security solutions addressing those requirements. We do not define what possible attacks an adversary may run in the DESEOS scenario in order to derive security requirements and corresponding security solutions mitigating those attacks. However, when validating security aspects of the DESEOS framework we will consider possible attacks an adversary may run but, in this case, DESEOS security properties are not affected but their fulfilment (and implementation) are.

For example, in the case of the DESEOS S&D artefact structure, if a protocol implementation is discovered to have some security flaws with potential security attacks, the corresponding fulfilment of the security protocol property will be replaced with a different protocol solution realizing this property.

Let us take the case of SSL/TLS security vulnerability issue on renegotiation[10], the DESEOS SRF would be set to either disable the renegotiation feature of TLS protocol implementations or use different protocol solutions for establishing and supporting confidentiality channel. In our case, WS-Security and WS-SecureConversation (part of Metro software package) could be used to fulfil the security protocol property when used for confidential channel providing message-level confidentiality instead of transport layer confidentiality as provided by the TLS protocol.

[10] `http://java.sun.com/javase/javaseforbusiness/docs/TLSReadme.html`

7 Relevant Project Activities on AAL

In this section we briefly revise some related project activities on AAL. AAL is a new ICT technology-based approach to provide support in daily life. Initially, AAL systems have focused on elderly and disabled citizens, but the concept is rapidly finding new applications that include other social groups and addresses other needs like socialisation, integration, etc. A good definition for current AAL systems can be found in [18]: "AAL aims to prolong the time people can live in a decent way in their own home by increasing their autonomy and self-confidence, the discharge of activities of daily living, to monitor and care for the elderly or ill person, to enhance the security and to save resources". Ambient Assisted Living is not just about technology and devices. In fact, it includes methods, concepts, (electronic) systems, devices as well as services that are providing unobtrusive support in daily life based on context and the situation of the person being assisted. In our vision, the future concept of AAL corresponds to a set of ICT technology-supported methods and processes that are oriented towards the enhancement of the quality of life of individuals.

In any case, the potential users of such technology do not form a homogeneous group. AAL users include individuals suffering from diverse disabilities and illnesses, wish to maintain an independent life at home, but also young and healthy individuals, who are mainly interested in "lifestyle functionalities" in order to improve their individual quality of life. Moreover, the assistance provided through AAL is not limited to the direct user. Products and services in the AAL environment will also address professional care provider, medical professionals as well as family members by providing better means of communication as well as easier social interaction.

A large number of AAL projects are currently active. Among these, we highlight the following ones based on their relevance and relation to DESEOS.

The goal of the ALADIN project[11] (Ambient Lighting Assistance for an Ageing Population) is to study the impact of lighting on the well-being and health of older people and translate this into a cost-effective open solution.

CAALiX[12] (Complete Ambient Assisting Living EXperiment) has as main objective to develop a wearable device able to measure specific vital signs of the elderly or infirm incorporating new sensors for fall detection and highly sensitive positioning.

EMERGE[13] (Emergency Monitoring and Prevention) focuses on the problem of excessive delays in calls to emergency medical services, which lead to an increased stay in hospital and the moving of elderly people into nursing homes, decreasing their quality of life unnecessarily and encurring considerable costs. The innovation is to track the patients' behavior via holistic approach detecting deviations from typical behavior patterns in order to preempt a health crisis as could be the case of strokes, falls or similar emergencies. The approach is to use unobtrusive sensors in the background to monitor activity, location and vital data.

The ENABLE[14] project aims to develop an user-centered enabling system for use by an elderly person in or out of the home. Main motivation is to mitigate the effects of any disability and to increase quality of life such as independence, autonomy, mobility, communications, care and safety. The aim of the project is to develop an open

[11] http://www.ambient-lighting.eu
[12] http://caalyx.eu
[13] http://www.emerge-project.eu
[14] http://www.enable-project.eu

and highly accessible reference architecture, to which subsystems and services can be seamlessly added according to the particular needs of elderly people and their careers.

The goal of the INHOME[15] project is to provide the means of improving the quality of life of elderly people at home by developing generic technologies for managing their domestic ambient environment, comprised of home appliances, entertainment equipment and home automation systems. The INHOME project focuses on the flexible use of appliances by selecting between experienced and inexperienced rather than enabled or disabled users.

NETCARITY[16] (NETworked multi-sensor system for elderly people: health CARe, safety and securITY in home environment) proposes a new integrated paradigm for supporting independence and awareness in elderly people living alone at their own home. The project fosters the development of a 'light' technological infrastructure to be integrated in homes of elderly people at a reduced cost and aims at the integration of micro and nano systems in a networked wireless/wired multi-sensing environment with plug and play capabilities and intelligent decision making for an effective detection of critical situations and help to complete tasks.

The OLDES (Older People's e-services at home) project[17] aims at developing a health care platform designed to make life easier for older people in their homes. The platform will be based on a PC corresponding to Negroponte's paradigm of a 100$ device, giving the guarantee of an affordable system. OLDES will provide: user entertainment services, through easy-to-access thematic channels and special interest forums supported by animators; and health care facilities based on established Internet and tele-care communication standards.

PERSONA[18] aims at developing a scalable open standard technological platform to build a broad range of AAL Services for social inclusion, for support in daily life activities, for early risk detection, for personal protection from health and environmental risks, for help with mobility and travelling at the cutting edge of devices aimed at assisting mobility.

SENSACTION-AAL[19] offers the opportunity for a significant advancement enhancing safety and security in balance and movement. The ultimate goal of the project is to enable older people to maintain independent mobility and daily life activities. The SENSACTION-AAL architecture will introduce new ICT solutions that make the proposed system: easy-to-wear and easy-to-use, active anywhere, anytime and cost effective.

UniversAAL[20] vision is that it should be as simple for users to download and setup AAL services as it is to download and install software applications on a modern operating system. UniversAAL will establish a store providing plug-and-play AAL applications and services that support multiple execution platforms and can be deployed to various devices and users. Finally the allocation of local human resources is also carried out by the store. UniversAAL aims to produce an open platform that provides a standardized approach making it technically feasible and economically viable to develop AAL solutions.

[15] http://www.ist-inhome.eu
[16] http://www.netcarity.org
[17] http://www.oldes.eu
[18] http://www.aal-persona.org
[19] http://www.sensaction-aal.eu
[20] http://www.universaal.org

The goal of SHARE-IT[21] (Supported Human Autonomy for Recovery and Enhancement of cognitive and motor abilities using Information Technologies) project is to develop a scalable and assistive technology so that elements can be modularly integrated into an intelligent home environment to enhance the individual's autonomy.

8 Conclusions and Future Work

Ambient Intelligence (AmI) is based on a vision of digital environments in which computing and communication technologies and devices help people in daily life through natural and intuitive interfaces and with an emphasis on improving their lives. Although this concept has been the subject of research in the past, it is only recently that the first promising results are appearing. In fact, when the concept of Ambient Intelligence was first introduced many scenarios considered to be too visionary or even science fiction. Despite the interest and research efforts devoted to the advancement of technologies that would enable the AmI vision to be realized in practice, we are still facing important challenges that require further investments in research and industrialization. One of these aspects, crucial for many AmI and AAL applications, is security.

In this paper we have presented the DESEOS system, designed to provide support for support children who must undergo frequent or long stays in hospital, with the objective of avoiding problems brought about by the changes in their routine and contact with their school environment and their family. The system targets two main aspects: (i) a comprehensive integration of security elements into an AAL system, thus demonstrating high levels of security and privacy for an AmI environment; and (ii) appropriate system design allowing it to be evolvable to adapt to changes in the context and scalable to handle communications between a large number of domains with their specific AmI environments.

The research that has guided the development of the DESEOS has been influenced by economic, psychological, social and pedagogical studies carried out by the multidisciplinary team of the DESEOS project, thus ensuring acceptance by end users. Nevertheless, we will carry out in 2011 an extensive evaluation of the technologies developed, from different points of view, and covering the different actors and users of the system.

From a technical point of view (the focus of this paper), our future work focuses on several specific milestones. In the short term, we plan to provide support for more certificate standards such as the SAML standard [12]. We also plan to extend the secure school integration scheme with single sign-on (SSO) pattern support. The implementation is currently under development based on openSSO[22], which in turn uses SAML protocol. This feature will fulfill important authentication requirements appearing when different school realms are linked in a larger school information network, as currently several schools of Andalucía region are. Additionally, in the mid term, we plan to integrate those new patterns into the actual implementation of the SRF collection of patters and test them in different AAL environments and devices. Extending the security solutions and integration schemes to non-java implementations is also part of the development plan. Finally, in a collaborative effort, the Hospital Clínico San Ce-

[21] `http://www.ist-shareit.eu/shareit`
[22] `http://opensso.org`

cilio in Granada (Spain) and several local schools are trying to integrate the DESEOS system in a real world setting.

References

1. M.J. Aguilar Cordero. *Influencia de la institucionalización y distintos modelos de acogida sobre el crecimiento, el desarrollo y el comportamiento en el síndrome de carencia afectiva en el niño.* PhD thesis, Universidad de Granada, 1995.
2. M.J Aguilar Cordero, G. Galdó Muñoz, A. Muñoz Hoyos, A. Molina Carballo, E. Vallejo Bolaños, C. Ruiz Cosano, and A. Valenzuela Ruiz. Valoración del nivel de ansiedad estado/rasgo en niños institucionalizados. In: IV Congreso Estatal Infancia Maltratada, 1995.
3. Alvaro Armenteros, A. Muñoz, A. Maña, and Daniel Serrano. Security and dependability in ambient intelligence scenarios: the communication prototype. In Jos Cordeiro and Joaquim Filipe, editors, *ICEIS (3)*, pages 49–56, Milan, Italy, 2009.
4. Juan M. Corchado, Javier Bajo, and Ajith Abraham. Gerami: Improving healthcare delivery in geriatric residences. *IEEE Intelligent Systems*, 23(2):19–25, March 2008.
5. Hristo Koshutanski and Fabio Massacci. Interactive access control for autonomic systems: from theory to implementation. *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, 3(3), 2008.
6. Johnny Chung Lee. Hacking the Nintendo Wii Remote. *IEEE Pervasive Computing*, 7(3):39–45, July 2008.
7. Maryanne Lockin. The redefinition of failure to thrive from a case study perspective. *Pediatric nursing*, 31(6):474–479, 2005.
8. A. Muñoz Hoyos. Influencia de la institucionalización sobre el crecimiento, desarrollo y comportamiento en el niño. Part of the course: Principales problemas sociales en la infancia. Educación y cuidados. Escuela Universitaria de Ciencias de la Salud. Granada, 1996.
9. A. Muñoz Hoyos. Problemática del niño institucionalizado. Part of the course: Pediatría Social. Universidad de Sevilla. Facultad de Medicina. Departamento de Pediatra. Sevilla, 2000.
10. J. Nehmer, Martin Becker, Arthur Karshmer, and Rosemarie Lamm. Living assistance systems: an ambient intelligence approach. In *Proceedings of the 28th international conference on Software engineering*, pages 43 – 50, Shanghai, 2006. ACM.
11. Boris De Ruyter. Ambient assisted-living research in carelab. *Interactions*, 14(4):30, July 2007.
12. SAML OASIS Standard. Security Assertion Markup Language (SAML). http://saml.xml.org.
13. Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Frank Buschmann, and Peter Sommerlad. *Security Patterns : Integrating Security and Systems Engineering (Wiley Software Patterns Series)*. John Wiley & Sons, March 2006.
14. D. Serrano, A. Maña, B. Gallego-nicasio, and A. Muñoz. Security Patterns, Toward a Further Level. In E. Fernández-Medina, M. Malek, and J. Hernando, editors, *SECRYPT*, pages 349–356. INSTICC Press, 2009.
15. Daniel Serrano, A. Maña, and Athanasios-Dimitrios Sotiriou. Towards Precise and Certified Security Patterns. In *DEXA Workshops*, pages 289–291, Turin, 2008. IEEE Computer Society.
16. G. Spanoudakis, A. Maña, and S. Kokolakis. *Security and Dependability for Ambient Intelligence (Advances in Information Security)*. Springer, 1 edition, 2009.
17. Frank Stajano. *Security for Ubiquitous Computing*. John Wiley and Sons, February 2002.
18. Dr. Horst Steg, Dr. Hartmut Strese, Claudia Loroff, Jérôme Hull, and Sophie Schmidt. *Europe Is Facing a Demographic Challenge Ambient Assisted Living Offers Solutions*. Ambient Assisted Living - European Overview Report, 2006.
19. Trusted Computing Group. Trusted Platform Module (TPM) Specifications. http://www.trustedcomputinggroup.org/resources/tpm_main_specification.
20. X.509. The directory: Public-key and attribute certificate frameworks, 2005. ITU-T Recommendation X.509:2005 | ISO/IEC 9594-8:2005.