SEVENTH FRAMEWORK PROGRAMME	**Project Acronym: GiraffPlus** **Project Title: Combining social interaction and long term monitoring for promoting independent living** **Grant agreement no.: 288173** **Starting date: 1st January 2012** **Ending date: 31st December 2014**

D2.1 First Prototype of sensors, Giraff platform and network system report

WP related to the Deliverable:	2
Nature:	P
Dissemination Level :	PU
Version:	Final
Author(s):	Filippo Palumbo (CNR-ISTI), Francesco Furfari (CNR-ISTI), Manlio Bacco (CNR-ISTI), Maria Lindén (MdH), Mats Björkman (MdH), Stephen von Rump (Giraff)
Project Participant(s) Contributing:	UMA, CNR-ISTI, Giraff, MdH,
Contractual Date of Delivery:	20121230
Actual Date of Delivery:	20121230

Document History

Version	Date	Type of editing	Editorial
0.1	07/12/12	Initial draft	CNR-ISTI
0.2		Updated version	
0.3		Complete version to be send to reviewers	
0.4		Revised version after comment of reviewers and consortium	
0.5		Final version	ORU

Disclaimer:

No confidential material is included therein.

Deliverable Summary

This document reports on the first prototype of the system deployed and installed at month 12 in the pilot apartment Ängen in Örebro. It is an integration of the information already reported in the Deliverable 5.1 which describes the preliminary technological integration achieved at month 9.
In addition to that deliverable this document provides a refinement of the initial system architecture according the feedback obtained during the implementation phase, and updates the status of development of the WP2. An analysis of security and privacy requirements regarding collecting, processing and transferring of personal information is also presented.

Currently the prototype includes the Giraff robot, the Look4Myhealth kit, the monitoring sensors from Tunstall, additional environmental sensors, a physiological sensor for pulse oximetry measurements based on Android, the context recognition and configuration planning modules, and the remote storage and repository to collect user data. An initial version of the middleware is also present. The final version of the middleware will be available at month 18 (Deliverable D2.2) when the development of the several modules composing the system is more mature and all the technical requirements completed.

Table of Contents

List of Figures

1 Introduction

1.1 Scope of the document

The document describes the first prototype of sensors, GiraffPlus platform and network system. An initial version of the system with simple monitoring sensors and an initial network infrastructure is descripted. This first prototype of the GiraffPlus ecosystem has been deployed at a test pilot site in Ängen that is located in Örebro, Sweden. The scope of the deployment is to provide a realistic environment where the GiraffPlus components can be tested in the context of the complete system.

The scope of the document is to briefly summarize the hardware components deployed at Ängen and the software components, as a detailed description of these components has already been presented in D5.1. In this document particular attention is given to the gluing component: the middleware. In addition the document presents an analysis of security and privacy requirements regarding collecting, processing and transferring of personal information.

1.2 Deliverable structure

The document gives first an outlined of what has been achieved and how it matches the DoW. In section 2 first an overall view then a detailed description of the main component, the middleware, is given. Section 3 explains how to use and install it. Then a brief summary of the hardware and software components deployed at the Ängen apartment is given. Finally an analysis of security and privacy requirements regarding collecting, processing and transferring of personal information is presented.

1.3 Deviations with respect to the plan

According to the DoW the first Prototype of sensors, Giraff platform and network system D2.1 is described as follow:

"An initial version of the system with simple monitoring sensors and an initial network infrastructure. Deployed at a pilot site. A report will describe the prototype."

A more detailed description is given in Task 2.1:

"Adapters' components, drivers, and gateway solutions will be developed in order to facilitate the discovery, access and control of such sensors in the Giraff+ system. The OSGi platform will be the reference platform to allow smooth integration of such components. Open source solution will be considered to integrate widespread technologies in the home automation domain, e-health entertainment and smart energy domain. State of the art technologies like Bluetooth and ZigBee will be mainly considered for body and local area networks but ad hoc solution will be developed for sensors not available on the market by using sensor platforms based on IEEE 802.15.4 standard."

The middleware currently deployed in the pilot site, the Ängen apartment, satisfies the requirements stated in the DoW and achieves the aims of facilitate the discovery, access and

control of the adapters' components, drivers, and gateway solutions by the monitoring services. In particular the Giraff robot, the Look4Myhealth kit and the sensors from Tunstall are deployed in the apartment and the data provided are available. Additional environmental sensors, a physiological sensor for pulse oximetry measurements based on Android, the context recognition and configuration planning modules, and the remote storage and repository to collect user data are also deployed in the apartment and are communicating via the middleware.

As the Task 2.1 said, the GiraffPlus system components can discover the presence of such devices installed in the environment using the lower levels of the middleware. Through the middleware buses it is possible to discover and access the sensors' services and their data. Other components of the system can also control the Giraff robot, the Look4Myhealth kit, and the sensors from Tunstall using a RESTful API exposed through the REST connector of the middleware.

The integration of a complete control API for these components is expected to be completed at month 18. By this deadline an ad hoc solution for sensors using platforms based on IEEE 802.15.4 standard will be developed and integrated satisfying the Sy1, Sy2, and Sy3 objectives described in the DoW.

The middleware has been developed using the OSGi platform as stated in the Task 2.1 of the Dow. However, some components of the GiraffPlus system have been developed using the C++ language. For those particular cases a C++ version of the middleware was preferred that was using the same connectors and exposing the same API to upper layers and was facilitating the integration of different services written in different languages. Any service can communicate with the others in a transparent way. Moreover an Android version of the middleware has been developed in order to integrate sensors based on that platform as reported in D5.1. A fully functional version of the C++ and Android flavor of the middleware is expected to be completed at month 18.

2 System Overview

2.1 The Revised System Architecture

The Giraff robot, the sensors, the services for the activity recognition, and the components integrated in the system will use a software infrastructure, which is based on a middleware that hides heterogeneity and distribution of the computational resources in the environment.

The actual GiraffPlus middleware solution uses a Java/OSGi platform as the reference platform for the development, however the integration of such components is demanding, especially if we consider that the system is composed of different services written in different languages and it may need to be accessible by a number of remote healthcare centers which may use different protocols. The fragmentation in this sector is still high, but there are initiatives working to build converging solutions. Service interoperability is a key point to build an ecosystem of applications that helps the growth of an AAL (Ambient Assisted Living) consumer market. In this regards, several European projects have intensely worked to the definition and standardization of a common platform for AAL, on top of which to develop intelligent software applications for the end users. Our objective is to design and develop a system compliant to the results of the most promising research projects in this field. The universAAL[1] project can be considered the major representative of this effort. It is an FP7 project aiming to standardize an open platform and reference specification for AAL.

Within the universAAL ecosystem, an AAL Space is intended to be the physical environment – such as the home of an assisted person – in which independent-living services are provided to people that need any sort of assistance. In such a virtual ecosystem, hardware as well as software components can "live" while being able to share their capabilities. In this space, the universAAL platform facilitates the sharing of three types of capabilities: Context (data based on shared models), Service (control) and User Interaction (view). Therefore, connecting components to the universAAL platform is equivalent to using the brokerage mechanisms of the universAAL platform in these three areas for interacting with other components in the system. Such connectors together with the application logic behind the connected component are called altogether "AAL Applications". Figure 1 shows the universAAL architecture.

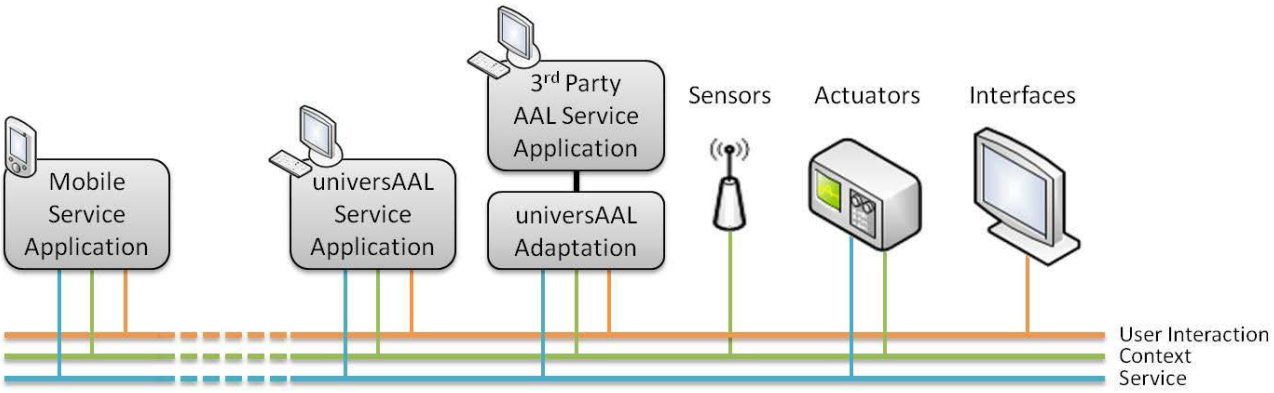


Figure 1 the universAAL architecture

As stated in the DoW, it is our intention to be aligned to the universAAL results, to reuse the Open Source software released by universAAL as much as possible, and to share the use cases based on the teleoperated robot system in order to enrich the universAAL platform with the

technological requirements deriving from our project. The concrete architecture currently implemented by GiraffPlus is mainly derived from the universAAL project that is based on the OSGi platform. However, as said in section 1.3, an effort to convert such system to a different language as C++ has been made.

The GiraffPlus middleware concrete architecture can be considered a "light" version of the universAAL reference architecture. In the GiraffPlus vision there is no need to offer the same amount of development and market support provided by the universAAL platform. Furthermore, in the GiraffPlus ecosystem is already present a Data Visualization, Personalization ad Interaction Services component that takes care of the user interaction capabilities of the overall system. The GiraffPlus middleware brokerage mechanism has a lighter set of capabilities: Context (to provide access to the data) and Service (to discover and control the services). Figure 2 shows the revised system architecture.

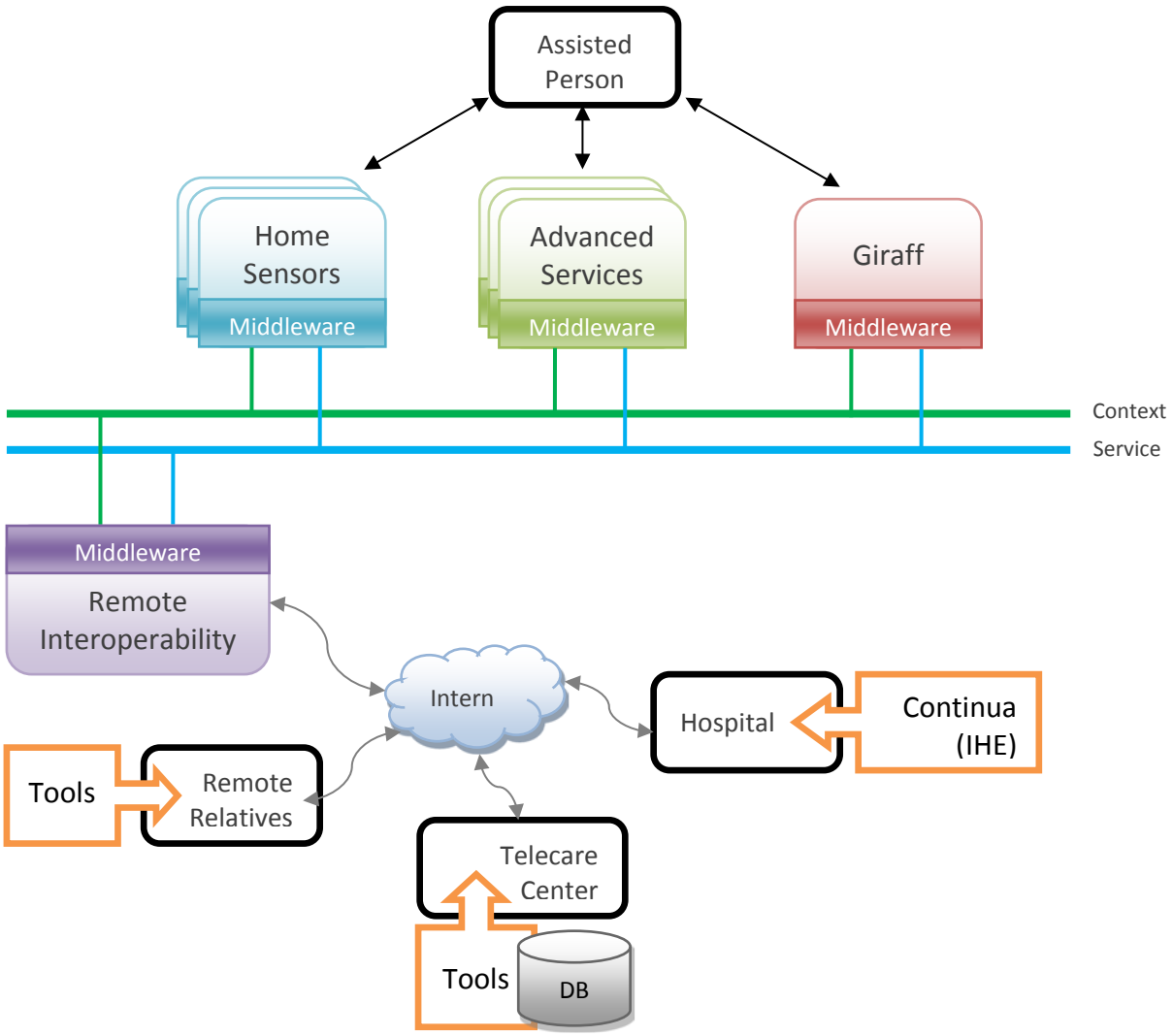


Figure 2 the GiraffPlus revised architecture

2.2 The Middleware

The middleware infrastructure present in Ängen has two layers: a core middleware API layer and a communication layer that includes a publish/subscribe connector and a RESTful connector. The middleware is written in Java, using the OSGi framework. OSGi technology is a set of specifications that defines a dynamic component system for Java. These specifications reduce software complexity by providing a modular architecture for large-scale distributed systems as well as small, embedded applications.

A generic service built upon the middleware can discover which sensors are present in the environment and other services with their functionalities using methods from the middleware API layer. The underlying layer fulfils these requests exploiting the connectors available. In the communication layer an MQTT [2] and a RESTful [3] connector are present. By mean of these connectors the middleware realizes a publish/subscribe and a methods description and invocation mechanism transparently to the services that use them.

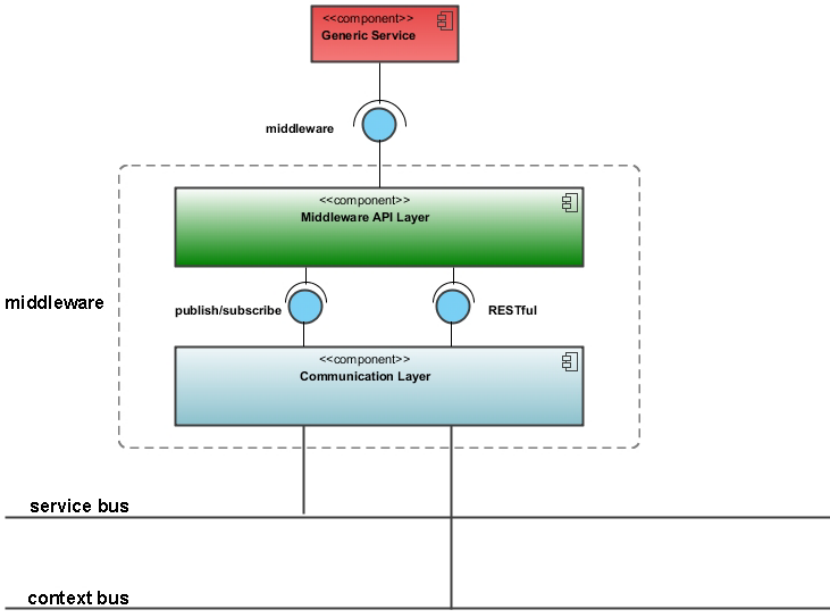


Figure 3 the GiraffPlus middleware layers

Two buses form the heart of the GiraffPlus middleware: a context bus and a service bus. All communication between applications can happen in a round-about way via one of them, even if physically, the applications are located on the same hardware node. Each of the buses handles a specific type of message/request and is realized by different kinds of topics.

The aim of the middleware is to provide a publish/subscribe mechanism for accessing the context information about the physical environment and physiological data. This information will be exposed as different topics:

- one topic for discovery and description of devices and services (Service Bus)
- one topic for context analysis (Context Bus)

In this way, the context bus is used to publish and retrieve events triggered by sensors and applications, while the service bus is used to discover devices and services. The middleware is in charge of presenting the available sensors and components in the system implementing an announce mechanism on a service bus. Once these resources are described in the service bus, a generic component can search for it, read its description and use it. The middleware takes care of dispatching information about the state of the resources among components by means of a context bus. Any component interested of monitoring these resources can subscribe to the relative topics. The topic used for discovery and description of devices and services, the so called Service Bus, has this kind of format:

```
/<<location>>/serviceBus/<<serviceType>>/<<category>>/id/
```

The message of this topic will be a description of the service or device. Any changes in a property status of a device or service will be published through the Context Bus. This kind of topic will have this format:

```
/<<location>>/contextBus/<<serviceType>>/<<category>>/id/
```

There could be a subtopic for each property changed. For each property there will a message in form of a JSON file containing a value, a timestamp, a previous value and a previous timestamp together with other information useful for configuration and identification. The context bus is also used by other system components in order to publish events triggered by some context analysis performed i.e. activities from an activity recognition reasoner.

2.2.1 The Middleware API

The API Layer is responsible to offer a simple set of functionalities to the services in order to fully exploit the middleware features. The OSGi bundle *giraff.middleware* is made-up of a set of interfaces and implementation classes that expose the following methods:

```
public void announce(Topic serviceBusTopic, Message descriptor);
```

This method is used by a service for announcing itself during the start-up phase. This is done by the middleware publishing a description of the service on the service bus. In this way any other component present in the system that is interested in such a service will be aware of it.

```
public Message[] search(String query);
```

This method is used by a service for searching for one or more resources (sensors or services) using a query by strings that represent topic filters. Topic filters can contain wildcards. With wildcards, a service can search for and obtain the description of different resources. The descriptor message object includes the information about the relative topic; in this way a service can subsequently subscribe to the topic to which it is interested in.

```
public void publish(Topic contextBusTopic, Message message);
```

This method is used by a service to publish messages on the context bus. A message is an object that includes fields relative to the status of a sensor or an activity processed by the service.

The message includes other information about the resource like id, previous status, timestamps, location and resource specific properties. It will be serialized as JSON file by the communication layer.

```
public void subscribe(Topic topic, Listener topicListener);
```

This method is used by a service to subscribe to topics in which it is interested. Any notification and message received will be handled by a listener. The topicListener is created by the service and registered to a topic to track the evolution of a topic. The topic can be already present in the system and discovered by a search or not present at the moment. In the latter case the service will be listening for a topic in which it is interested even if it is not present at the moment. As soon as the topic, as a resource or service, is announced on the service bus, the topicListener registered by the service will be notified.

```
public void registerAsService(String interfaceName, Object
implementationClass);
```

This method is used by a service when it wants to register its RESTful interface in the system. The registerAsService method calls the RESTful connector api from the bottom layer to make available the service in the system. In this way any other service in the system, after discovering it, can use it. The description of the interface to be registered is stored in the Descriptor file announced when the service is started.

```
public void invoke(String serviceName, String method, String[] values,
Listener serviceListener);
```

This method is used by a service that wants to invoke a method from another service previously registered as service in the system. The return value of the method will be handled by a listener. Figure 4 shows the main classes of the bundle.

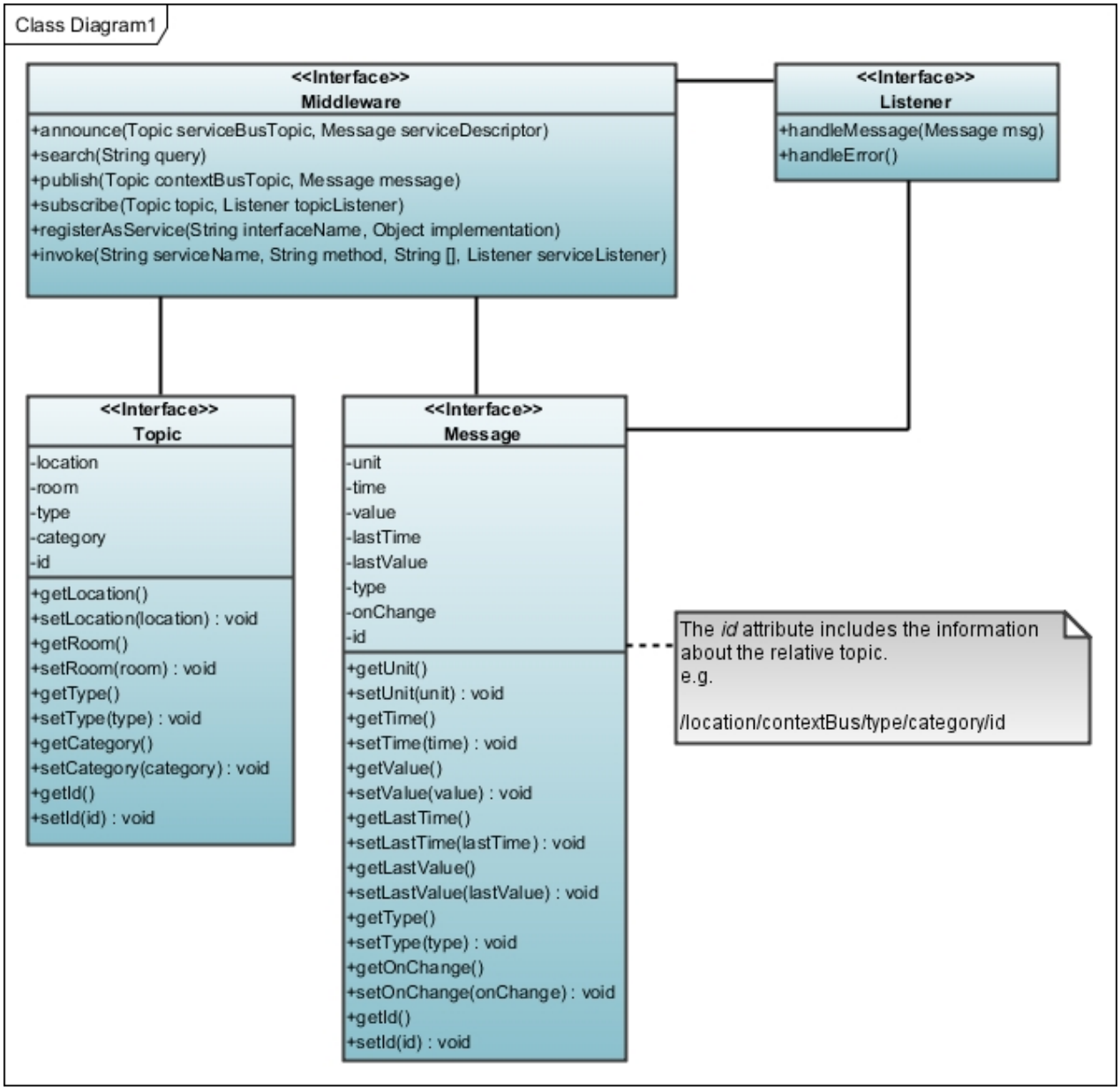
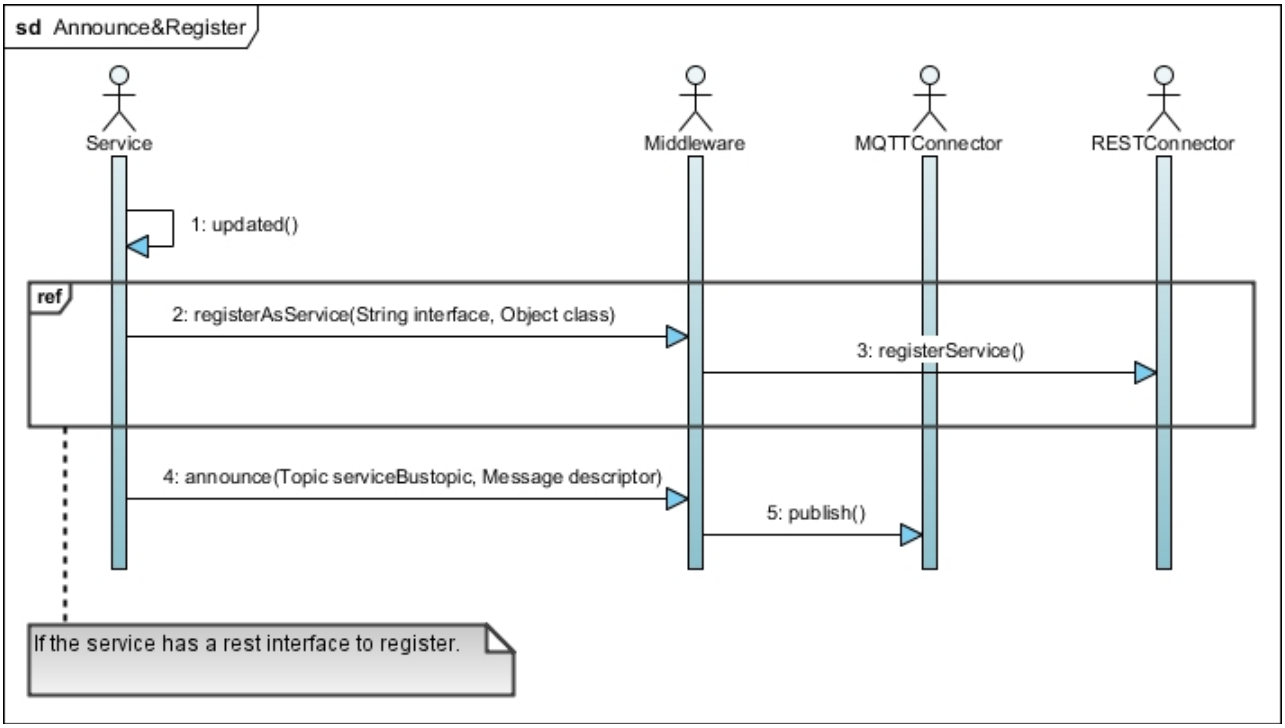


Figure 4 the class diagram of the giraff.middleware package

The main workflows for announcing, registering, discovering, and invoking of resources are detailed in the sequence diagrams shown in Figure 5.



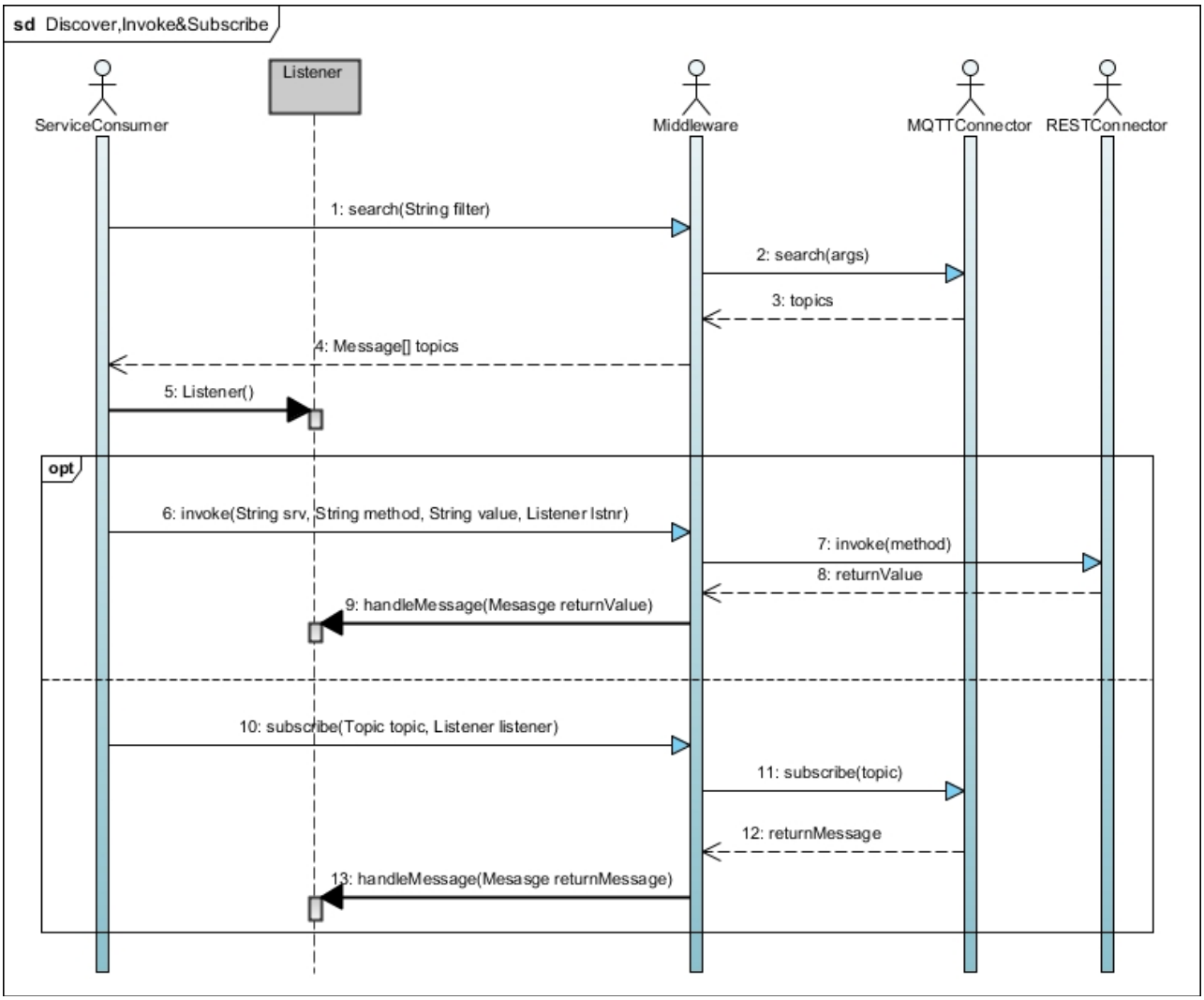


Figure 5 the sequence diagrams for announcing, registering, discovering, and invoking

2.2.2 The Communication layer

The communication layer is responsible of the implementation of all the mechanisms hidden by the upper layer of the services. The publish/subscribe and the RESTful patterns are realized by mean of connectors. These connectors are realized as two OSGi components that made up the communication layer: the *giraff.mqtt* and the *giraff.rest* bundle.

The technology used to realize the publish/subscribe pattern is MQTT. MQTT stands for MQ Telemetry Transport. It is a lightweight publish/subscribe protocol flowing over TCP/IP for remote sensors and control devices through low bandwidth, unreliable or intermittent communications [2]. The middleware implements this technology by using an OSGi bundle that publishes any event and description from sensors and services to the previously descripted dedicated topics (service and context bus). The topics are managed by an external broker.

The RESTful connector is a module that allows other system components to set and retrieve the properties of the devices present in the environment through a RESTful API (GET, PUT, POST, and DELETE) [3]. Through this API will be possible to invoke methods of a service that it has previously registered its interface to the middleware. A middleware instance will have a webserver that exposes the interfaces registered by the services. The technology used to implement this mechanism is Apache CXF [4]. Apache CXF is an open source services framework used to build the restful service by mean of frontend programming APIs like JAX-RS. The component of this framework used to set up the webserver on each node is Jetty. A service deployed on any middleware instance will be able to access any resource by mean of a network load balancing mechanism. An *httpd* [5] server will be used for this scope. Since the MQTT technology requires a broker server to store and manage the topics, a network load balancing service will be implemented upon the same device.

Figure 6 shows the deployment diagram of a generic environment with two middleware instances and two services installed upon it.

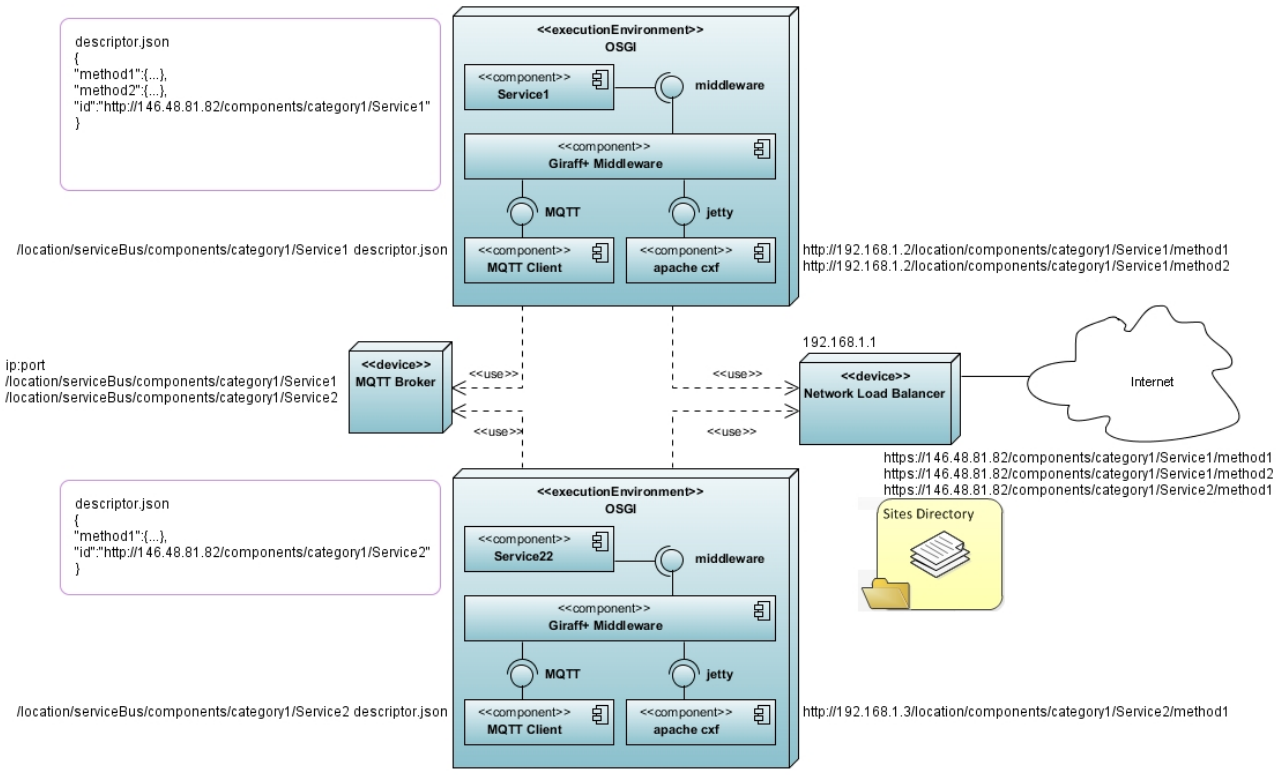


Figure 6 the deployment diagram of an example scenario

2.3 Main Components

The GiraffPlus system is composed of several hardware and software components. Hardware components like sensors and actuators (Tunstall, Intellicare, and Giraff Robot) have been integrated in the system by mean of services that uses the middleware API. Software components like the Data Storage and the Intelligent Monitoring and Adaptation Services has been integrated by mean of the use of the same communication connector (MQTT). They can interact with the middleware using the Middleware API Layer.

2.3.1 Tunstall Service

Tunstall sensors described in section 4.2.2 have been integrated by mean of a service exploiting the middleware interface. The component wraps the native command of the USB Tapit through JNI code. The USB Tapit listens for events from sensors and sends it to the COM port. The Tunstall service associates the events with the relative sensor and publishes the messages to the context bus through the MQTT connector. The service is implemented as an OSGi bundle named *giraff.services.tunstall* and it can be accessed through the svn repository descripted in the code management section. To properly use the component, the sensors must be first configured on the Connect+ Gateway. All the configurations are stored in a configuration file *config.ini* in the config directory present in the bundle. Figure 7 shows the component diagram of the current integration.

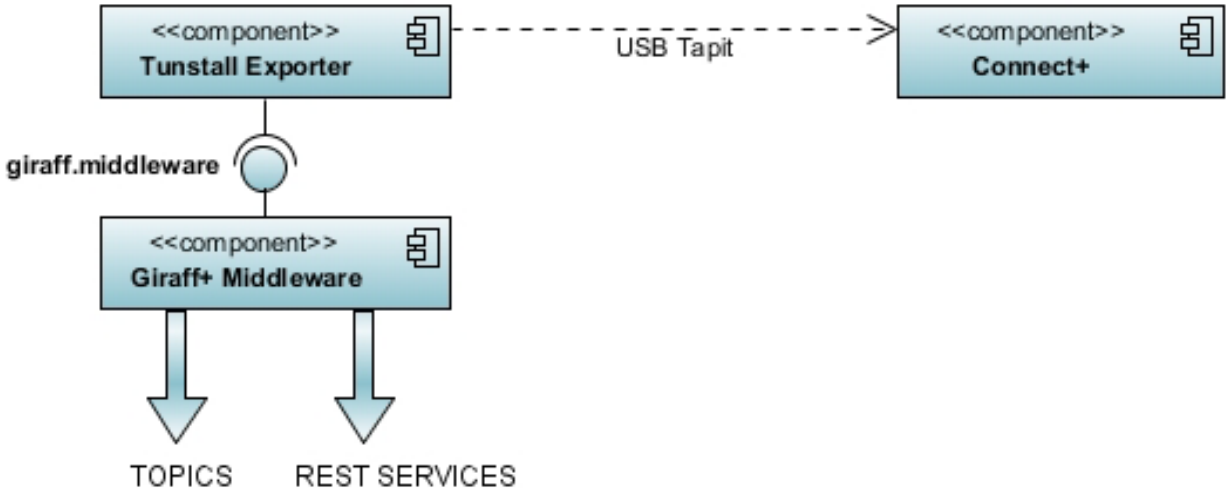


Figure 7 the component diagram for the Tunstall service

2.3.2 Intellicare Service

The Intellicare kit described in section 4.2.1 has been integrated by mean of a service exploiting the middleware interface. The component wraps the API (OneCareDataAccessV1API) exposed by the Intellicare server by mean of a RESTful service registered in the system using the REST connector. Any other service present in the environment will be able to call this API and get data locally without access directly the Intellicare server. This is possible because the service publish the description of the RESTful methods on the service bus in the announce phase. In this way any interested service can learn about the methods invocation mechanism reading the Intellicare service descriptor. The service is implemented as an OSGi bundle named

giraff.services.intellicare and it can be accessed through the svn repository descripted in the code management section.

The current available methods are:

- getMeasurementsByPeriod(int group, long date, int periodType);
- getLastActiveAlarms(int num);
- getLastAlarms(int num);
- getSystemInformation();

Figure 8 shows the component diagram of the current integration.

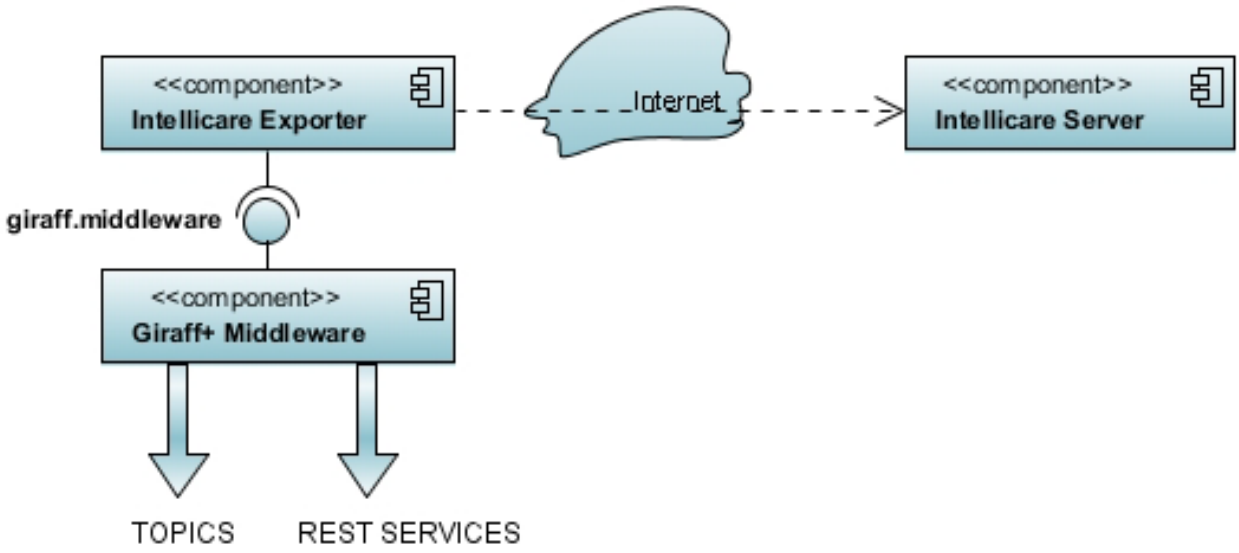


Figure 8 the component diagram for the Intellicare service

2.3.3 Android Service

In the GiraffPlus ecosystem there are some sensors and components based on mobile execution environments. A pulse oximeter sensor and an acceleration sensor combined into a monitoring system based on a smart-phone android device are available in the apartment for the user evaluation. This component is explained in details in section 4.2.3. A mobile component in the system can publish data via an android application. This application can interact with the GiraffPlus system through an android version of the middleware that mimics the behavior of the standard middleware installed on the fixed nodes.

The core component of the android version of the middleware is an android service called *giraff.android* and it can be accessed through the svn repository descripted in the code management section. The GiraffPlusService exposes an API that is a subset of the standard API from the Middleware API Layer. Figure t shows the class diagram of the GiraffPlusService. A generic android application in the GiraffPlus ecosystem is supposed to only announce itself as a resource and publish messages about the sensors states because of the limited resources of a mobile platform in terms of battery life.

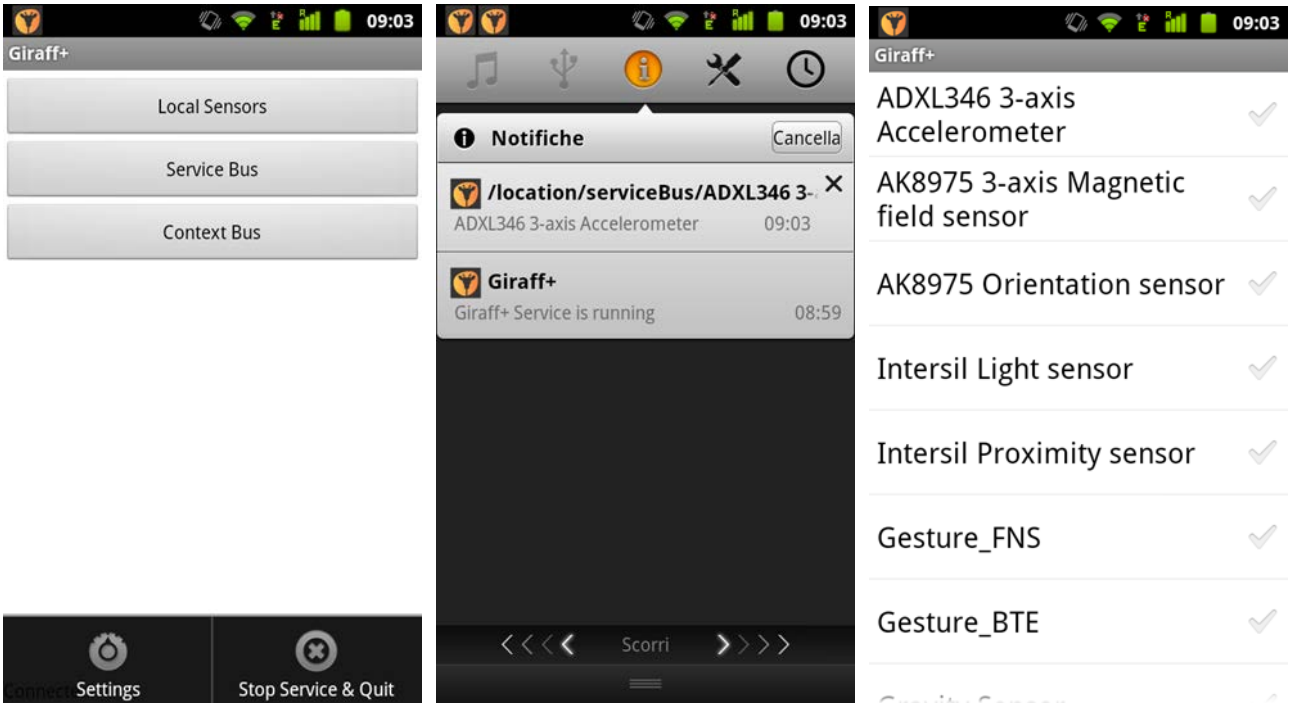


Figure 9 an example application that uses the GiraffPlus android service

The GiraffPlus middleware service is meant to be long-running, however if the phone gets low on memory, typically because the user is using an app in the foreground (therefore is treated as high priority) which needs a lot of memory, it will be killed. To avoid this the GiraffPlus service return the START_STICKY constant when the service is started, if the Android system has to kill the service to free up valuable resources, then the service needs to be restarted when resource become available again.

To use the service a generic application is needed that can integrate it using a Binder [6] interface offered by the Android system as shown in Figure 9.

2.3.4 Other Components

Software components described in section 4.3 like the Data Storage and the Intelligent Monitoring and Adaptation Services has been integrated using the same communication connector (MQTT). They can interact with the middleware using the Middleware API Layer.

The Data Storage service plays an important role in the overall architecture since it offers to other services a way to access historical data through an API registered on the system. Any topic present on the buses is subscribed by this component and any message published is stored in the database.

The Intelligent Monitoring and Adaptation Services together with the Context Recognition and Configuration planner exploit the middleware functionalities using connectors implemented with the same technologies but in a different language (C++). In this way a C++ version of the middleware is realized.

3 Software Development

3.1 Code Management

The code presented in the previous sections is organized and maintained on a SVN server. A SVN (Subversion) Server has been set up at the beginning of the project and has proved to be a fundamental instrument for the management and sharing of project data. SVN allows for the concurrent management of (different versions of) files and it proved very valuable for the project: software and documents (e.g. tutorials, guides and publications) are now routinely and effectively managed, shared and jointly edited via SVN by the XLAB personnel.

The SVN is accessible by all the partners at the following link: https://giraff.xlab.si/svn/giraff/src. The repository is composed by a set of folders that reflect the work packages partition. Concerning the WP2 code, it is partitioned reflecting the main component analysis made in the previous section. The following shows the hierarchical view of folders:

```
\src
   \WP2
      \Android
      \C++
      \OSGi
         \giraff.services.intellicare
         \giraff.services.tunstall
         \giraff.middleware
         \giraff.mqtt
         \giraff.pom
         \giraff.rest
         \giraff.tester
         \rundir
      \util
   \WP3
   \WP4
\WP5
```

3.2 Configuration and Installation

The code described in this document has been written in OSGi. The OSGi framework (Open Services Gateway initiative) is a module system and service platform for the Java programming language that implements a complete and dynamic component model. Applications or components (coming in the form of bundles for deployment) can be remotely installed, started, stopped, updated, and uninstalled without requiring a reboot. Application life cycle management (start, stop, install, etc.) is done via APIs that allow for remote downloading of management policies. The service registry allows bundles to detect the addition of new services, or the removal of services, and adapt accordingly.

Concerning the project management, Apache Maven has been chosen as a tool. Apache Maven is a software project management and comprehension tool. Based on the concept of a project object model (POM), Maven can manage a project's building, reporting and documentation from a central piece of information. Maven uses an XML file to describe the software project being built, its dependencies on other external modules and components, the building order, directories, and required plug-ins. It comes with pre-defined targets for performing

certain well-defined tasks such as compilation of code and its packaging. Maven dynamically downloads Java libraries and Maven plug-ins from one or more repositories such as the Maven 2 Central Repository, and stores them in a local cache. This local cache of downloaded artifacts can also be updated with artifacts created by local projects. Public repositories can also be updated. Maven is built using a plugin-based architecture that allows it to make use of any application controllable through standard input. Maven projects are configured using a Project Object Model, which is stored in a pom.xml file.

In order to run the middleware a tester bundle has been implemented: *giraff.tester*. Before trying to execute GiraffPlus Middleware, it must be check if all the following requirements are satisfied.

- Hardware Requirements

  GiraffPlus Middleware requires a PC with compatible hardware (USB Tapit) to use the Tunstall service otherwise the service will not be available. The USB Tapit must be installed and configured via the Lifeline Connect+ gateway. A file called triggers.EE is in the util dir. That is a sample configuration file that can be used if the same devices (fall detector, PIR presence detector, universal sensor with bed presence/absence detector, mains power outlet, personal trigger, and LL Connect+ buttons) are used. The file can be loaded from the PCConnect software, included in the same dir.

- Software Requirements

  GiraffPlus Middleware doesn't require any special software except for Java 5 (or Java 1.5+), OSGi 3 compliant framework and Apache Maven.

- Obtain the code

  The source repository used by GiraffPlus Middleware is Subversion, you will need SVN tool in order to get the code. The system is also configured for using Maven for the creation and set-up of an OSGi environment. In this way, testing the project becomes easy also for non-OSGi expert. It is worth to note that the creation of the OSGi environment is based on Pax Runner which downloads on demand all the OSGi bundles related to the execution environment.

After these preliminary steps it is possible to build from the source following these instructions:

1. Download the development branch from https://giraff.xlab.si/svn/giraff/src/WP2/OSGi, for example launching the command

   ```
   svn co https://giraff.xlab.si/svn/giraff/src/WP2/OSGi GiraffPlusMW
   ```

2. Move to GiraffPlusMW\giraff.pom and launch the following command to build the whole project:

   ```
   mvn install
   ```

3. Move to GiraffPlusMW\giraff.tester and create the OSGi environment using the command

```
mvn pax:run
```

A new sub-directory, named 'runner', is created.

4. Launch GiraffPlusMW\giraff.tester\runner\run.bat to start-up the OSGi environment

The script runs version 2.0.2 of the Felix OSGi environment. The OSGi environment will be loaded with a terminal console, with the following bundles:

```
-> ps
START LEVEL 6
   ID   State         Level  Name
[   0] [Active     ] [    0] System Bundle (2.0.2)
[   1] [Active     ] [    5] Commons Codec (1.4)
[   2] [Active     ] [    5] OSGi R4 Core Bundle (4.1)
[   3] [Active     ] [    5] OSGi R4 Compendium Bundle (4.1.0)
[   4] [Active     ] [    5] Apache Felix Configuration Admin Service (1.2.4)
[   6] [Active     ] [    5] Apache Felix EventAdmin (1.2.14)
[   7] [Active     ] [    5] mqtt-client (1.2)
[   8] [Active     ] [    5] hawtbuf (1.9.0)
[   9] [Active     ] [    5] hawtdispatch (1.11.0)
[  10] [Active     ] [    5] hawtdispatch-transport (1.11.0)
[  11] [Active     ] [    5] Distributed OSGi Distribution Software Single-
Bundle Distribution (1.2)
[  12] [Active     ] [    5] JSON.simple (1.1.1)
[  13] [Active     ] [    5] giraff.rest (1.0.0.SNAPSHOT)
[  14] [Active     ] [    5] giraff.mqtt (1.0.0.SNAPSHOT)
[  15] [Active     ] [    5] giraff.middleware (1.0.0.SNAPSHOT)
[  16] [Installed  ] [    5] giraff.services.tunstall (1.0.0.SNAPSHOT)
[  17] [Installed  ] [    5] giraff.services.intellicare (1.0.0.SNAPSHOT)
[  18] [Active     ] [    1] Apache Felix Shell Service (1.4.1)
[  19] [Active     ] [    1] Apache Felix Shell TUI (1.4.1)
->
```

Now it is possible to start manually some OSGi bundles. This helps to have a clear perspective of what it is running. Generally OSGi supports the following syntax in order to start a bundle:
`start <id>`
where <id> is the number of the bundle. The <id> can be easily obtained listing the bundles:
`ps (or as alternative lb)`
It must be noted that the <id> of the bundles can be different from the ones presented here.

It is important to not forget configuring the OSGi environment. The system implemented uses the Apache Felix Configuration Admin Service to manage the configuration parameters of the bundles. The OSGi Compendium Configuration Admin Service specifies a service, which allows for easy management of configuration data for configurable components. Basically configuration is a list of name-value pairs. Configuration is managed by management applications by asking the Configuration Admin Service for such configuration. After updating the configuration, it is sent back to the Configuration Admin Service. The Configuration Admin Service is like a central hub, which cares for making persistent this configuration and also for distributing the configuration to interested parties. One class of such parties is the component to be configured. This is registered

as ManagedService service. There is also a notion of ManagedServiceFactory, which allows for multiple configurations of the same kind to be applied.

Thus, to properly configure the Tunstall service, properties like COM port, mode and timeouts must be set in a properties file that the Configuration Admin Service uses for the management. This file is located in the rundir/confadmin/services folder. For each service and component there is a configuration file named with the same package name followed by the suffix *pid.properties*:

```
\src
   \WP2
      \OSGI
         \rundir
            \giraff.services.intellicare.pid.properties
            \giraff.services.tunstall.pid.properties
            \giraff.middleware.pid.properties
            \giraff.mqtt.pid.properties
            \giraff.rest.pid.properties
```

When the configuration is done it is possible to start a particular service with the start command followed by the relative id. In the case of the Tunstall service when it is started any configured Tunstall device will be first published as a service bus topic with its descriptor file. Then, any event from sensors will be published as a message on the context bus topics.

4 Ängen Pilot Site

The test apartment Ängen is located in a unique building complex as part of an initiative to provide complete care facilitates for older people in Örebro, both elderly and independent seniors. The building complex includes Senior living and Partially Supported Living.
The Ängen apartment and the hardware and software components deployed has been described in details in the deliverable D5.1. In the following we summarize the hardware and software components deployed in the apartment and communicating via the middleware.

4.1 Hardware components

The hardware components that are currently deployed in the Ängen apartment are the following:

Intellicare kit

The sensors provided by Intellicare are sensors for blood pressure monitoring, glucose level measurements, temperature measurements, weight measurements and oxygen saturation measurements. In the version currently available at the apartment, the sensors connect to a gateway provided by Intellicare and transmit data to the Intellicare server. The data can be easily accessed via internet and are visible at the apartment via a computer. The data from Intellicare are also available to the rest of the GiraffPlus system via an alternative gateway based on an android platform as described in D1.3. The system is called Onecare and it is composed by one tablet pc with an Android based OneCare app. One of the components of OneCare is the “Data router”. This component is in charge of distributing data across multiple systems, eventually, changing data formats and ensuring proper authentication. The data collected by OneCare can be accessed using two methods. The data can be pulled from the system, allowing access to current and historical data. In particular it allows querying the database of measurements and get data or graphics of data so that they are presented to users. The other method to access the data is via data forwarding towards the GiraffPlus middleware. In this case the data are sent when they are acquired by the sensors. This method supports a publish/subscribe model. The middleware receives data from the platform and publishes it allowing all other components to access them. Other components can access the data from the sensors by subscribing to the topics that the middleware publishes.

The sensors available in the apartment are placed in the bathroom and are the following:

- The *blood pressure monitor*
- The *glucose meter*
- The *thermometer*
- The *weight scale*

Android physiological and inertia sensor

A pulse oximeter sensor and an acceleration sensor combined into a monitoring system based on a smart-phone android device are available in the apartment for the user evaluation. The

system publishes data via an android interface and using the GiraffPlus middleware store the data in the GiraffPlus database where they are accessible to the rest of the system.

The Tunstall sensors

The Tunstall sensors that are currently available in the apartment together with an indication where they are places are listed below.

Bedroom

- The main gateway for the Tunstall sensors, Connect+.
- A sensor for *detection of body fluid sensors* (*enuresis sensor)*. The sensor is placed between the mattress and the sheet, and provides a warning on detection of moisture.
- Two *fall sensors*, either worn around the wrist or waist. The sensors raise an alarm in case of a fall. If normal activity is detected after the fall, the alarm can be canceled.
- One *Bed Occupancy Sensor*, using this sensor, the presence of a person can be determined.

Kitchen

- One FAST Passive InfraRed motion detector (PIR).

Living Room / Entry Hall

- One FAST Passive InfraRed motion detector (PIR).
- A wireless *Smoke detector* that alarms if smoke is detected. It also provides auto low battery reporting.

Living Room / Main

- One FAST Passive InfraRed motion detector (PIR).

Bathroom

- One flood detector.

Tunstall sensors are integrated in the system by exposing a data port on the Tunstall gateway (Connect+ social alarm) in the physical environment through a USB dongle named the Tapit USB. The data are primarily alerts raised by the sensors. To facilitate the integration, the middleware uses a wrapper that exposes the devices to the hardware abstraction layer.

Other components can access data from sensors by subscribing to the topics that the middleware will publish.

Additional sensors available at the apartment

There are five custom made sensory platforms in the apartment. They can be moved around easily and each one measures all (or a subset) of the following environmental parameters:

- Temperature (Ambient temperature or object temperature, e.g. a water pipe)
- Luminosity (Visible light level)
- Pressure (Can be used to determine if someone is sitting in a couch etc.)
- Passive Infrared (Motion in the room)

- Gap (Measures if an “optical gap” is occluded, which can be used to determine if a door is open etc.)

Currently, three of these sensors are in use, their position and main purposes are provided in the following table:

Location	Relevant sensors / Purpose
Bathroom	• Motion • Temperature on the warm-water pipe (in order to determine when water is used for showering)
Living room	• Motion • Pressure in the couch (to determine occupancy)
Kitchen	• Motion • Occlusion of a door sensor (Determines if the kitchen door is open or closed).

The sensors’ data are currently stored in the GiraffPlus database via the GiraffPlus middleware and are currently used by the context recognition module also installed in the apartment.

Giraff robot

The Giraff robot in Ängen is the latest version of the robot (3.3 version) that meets the technical requirements for the GiraffPlus project including the new motherboard, solid-state hard drive and more accessible electronics. These improvements are designed to allow for third-party application development including the auto-navigation features planned for the project. This unit also has a prototype of the new touch screen display, fully functional with the Windows drivers installed. The Giraff robot operates in the environment using a two way communication with the virtual visitor, allowing the robot to be evaluated by the end users in the context of the GiraffPlus system. A first integration of the Giraff robot has been done and events like level of battery can be published via the middleware. This information is important for the configuration planner as it gives an indication of the availability of the robot.

4.2 Software components

In the following the software components that are currently present in the Ängen apartment are listed. A more detailed description is provided in D5.1 and in D3.1.

Remote Access

The following components are implemented and present in the Ängen apartment to insure a secure remote access to the data.

- VPN Configuration: is used to establish a remote connection with the test sites to support update of software and resolving possible problems. Its biggest benefit is the possibility to keep a persistent connection with the outside server. Even with the network outages, the VPN connection re-establishes automatically after the

network problems have been fixed. This makes VPN ideal for the administration purposes. For establishing a VPN connection the OpenVPN application is used.

- ControlTier: the deploying package containing GiraffPlus local middleware software on remote machines is done using ControlTier. ControlTier is an open source, cross-platform deployment automation framework that helps to coordinate and scale service management and administration activities across multiple nodes and application tiers

- Data storage: it is used for long-term storage of data collected by physical services, as well as the data produced by other components (monitoring and adaptation services, interaction and personalization services). Additionally, it stores configuration data (sensor data, security restrictions, …) and logging data from all the software components in the system (all logs will be centrally available, and therefore it will be easier to maintain and debug the system). A cloud-based storage system is used running on the cloud infrastructure provided by XLab. It consists of three components: the database, the middleware listener and a RESTful service.

- Database: a MongoDB database is used which is flexible, scalable and can handle large volumes of data. For the Ängen apartment (as well as all future GiraffPlus equiped apartments) all stored data are automatically replicated among prepared MongoDB instances (replica-set), which provide automatic failover and automatic recovery (disaster recovery) of member nodes..

Intelligent Monitoring and Adaptation Services

Two modules that provide intelligent monitoring and adaptation services have also been deployed in the Ängen apartment and are now integrated. They are described in more detail in D5.1 and in D3.1.

- Context recognition: the system is able to infer context from sensory data represented as intervals on different timelines. It retrieves the sensor data from the GiraffPlus data storage via the middleware and it stores the recognized activities back in the data storage where they can be retrieved by the visualization and personalization module.
- Configuration planner: The configuration planner takes as input a set of models of available functionalities (which can be sensor devices, actuation devices, or computational processes), an current world state, and a set of goals in terms of state variables that should be observed (information goals, achieved by sensing and processing of sensor data) or should be set to a specific value (causal goal, achieved by actuation). It then produces solutions where each step in the plan is a configuration, i.e. a collection of communicating functionalities, and where there are causal dependencies between configurations. The domain model of the configuration planner, including models of sensors and actuators, is represented in JavaScript Object Notation (JSON) files. JSON is also used by the MongoDB database.

5 Security and privacy regarding collecting, processing and transferring of personal information

Personal information refers to all kinds of information that directly or indirectly can be attributed to a living, individual physical person. Also coded information is regarded as personal data as long as a code key exists.

Protecting personal information becomes a crucial issue when dealing with Clinical Information Systems or Patient Data Management Systems such as the GiraffPlus system. Assuming the amount of medical data which is expected to be collected, stored, processed and transferred by the system, we need to be able to guarantee that all these procedures are implemented according to the official regulations provided by European authorities and by the local laws in the countries involved, respectively. The local laws are to a large extent harmonized to the European regulations.

5.1 Overview of laws and regulations in Europe

The main source of information regarding this issue is a Data Protection Directive, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of the individuals with regards to the processing of personal data and on the free movement of such data [7], which regulates the processing of personal data within the European Union. It is an important component of EU privacy and human rights law. This directive has been transposed to national data protection legalisation across the EU.

The introduction of eHealth into daily medical practice changes the traditional model with pre-known entry points of patient data. The lack of legal certainty in the use of eHealth is well recognised. A study was performed between January 2006 and May 2007 regarding the European Community legalisation, with respect to various Directives. The result from this study is presented in the report Legally eHealth. Putting eHealth in its European Legal Context [8], there especially the challenges of compliance with rules of data protection and privacy, questions of product and services liability, and on the role of EU Competition laws on the development of eHealth industry within the European market are studied. The report aims to give an overview of the current EU level legalisations, although do not claim to give the legal answers. Further, case vignettes are given for a better understanding. The present report summarizes some parts of these results, especially treating data protection and privacy.

A new EU data protection law is under preparation, and a draft is presented by the m law group [9]. It provides for a harmonization of the data protection regulations throughout the EU, thereby making it easier for US companies to comply with these regulations.

5.2 What does the Swedish laws and regulations mean?

The Swedish legislation is particular important because Sweden is one of the country participating in the project and where test sites are going to be established. It has also one of the strictest regulations in Europe in this area and therefore it is an important point of reference for the project.

The website of CODEX, Centre for Research Ethics & Bioethics provides an overview of the laws regulating the handling of personal information in Sweden [10]. These are first and foremost the Personal Data Act (PUL) [11] and the Personal Data Ordinance [12], complemented by the Swedish Data Inspection Board's Authority Regulations [13]. The Public Access to Information and Secrecy Act (Offentlighets- och Sekretesslag) [14], Public Access to Information and Secrecy Ordinance (Offentlighets- och Sekretessförordning) [15] and Tryckfrihetsförordningen (regarding freedom of press) [16] are also essential. For health and medical services, the Law regarding health data registers (Lag om hälsodataregister) [17] and the Law on Patient Data (Patientdatalagen) [18] regulate how patient data is handled. The Law on Patient Data together with the service National Patient Overview (Nationell Patientöversikt, NPÖ) [19] are important and has made it possible to share documentation between care provides with the consent from the patient. Certain matters can be treated both in the Personal Data Act (PUL) and in the Law on Patient Data. In this case the Law on Patient Data overrule PUL. The National Board on Health and Welfare has issued accompanying regulations on "informationshantering och journalföring i hälso- och sjukvården" [20].

The following information is provided by the website of CODEX about the Personal Data Act [11]:

"The Personal Data Act (PUL) governs how data are used. According to PUL, the person in question is to be informed as to which information will be used. A person who submits information to a personal register established for research purposes has a further right to resulting information regarding him or herself. If a person can be identified - registers can also be anonymous - he or she also has the right to demand that incorrect or incomplete information be corrected or completed. The researcher should inform the subject on this issue. It is common that the responsibility to uphold good register practice lies with the research department's chairperson or president.

According to the principal rule in 10§ of the Law regarding Personal Information, the handling of personal information requires consent from the person in question, with an exception for certain "necessary considerations". For example, handling of information can be seen as necessary if it concerns a task of public interest. However, if sensitive information is involved, such as information on race or ethnic origin, political opinion, religious or philosophical conviction, membership in a union, or health or sex life, stricter demands apply. According to 19§ of the Law, handling such information for research requires approval from a research ethics board. It will judge research according to the Act on ethical review, which says that research can only be approved if it is performed with respect for human dignity, that human rights and freedoms always should be considered and that the welfare of subjects always trumps the needs of society and science. Risks shall always be balanced by scientific merit. Use of sensitive information for statistical purposes must be necessary as described in PUL 10§, and the interest to society must clearly outweigh the risk to an individual's integrity that handling of information can involve.

Note also that, according to 36§ of the Law and 10§ of the Regulation, certain types of research projects have an obligation to notify the Swedish Data Inspection Board. In other cases it is normally enough that the personal information representative be informed. One who, alone or in a group, decides on the object of and means for the handling of personal information is called the personal information officer (as a rule, this is an organisation), whereas the physical person appointed by the officer to ensure that personal information is handled correctly and according to

the law is the representative. For more on personal information in research, see advisory documents issued by the Swedish Data Inspection Board. The Board has also given out Answers to Consultation Concerning, for example, who is to be regarded as Controller of Personal Data in Connection with Clinical Studies.

Confidentiality in healthcare and in the social and behavioural sciences

As noted, a condition to be met for personal information from, e.g., patient journals to be released for research purposes is that the release be consistent with relevant provisions regarding secrecy, etc. However, consent from the concerned individuals always trumps secrecy rules.

In healthcare, information regarding health status and other personal matters are classified as confidential, if it is not obvious that it can be disclosed without any harm to the patient and his or her relatives. The individual's subjective opinion is important in deciding whether someone may be harmed. Secrecy is the professional confidentiality in public service for those who have access to information that may harm patients (or the safety of one's country, or public economic interest, etc.). The significance is that outsiders shall not gain access to information that has been designated confidential. This prohibition of disclosing confidential information pertains to oral reports, the release of public records or any other means of information transfer.

There are various exceptions. For research purposes, patients' journal information can be released with reservations. If you work at a public authority, you can assume the confidentiality already in place at the releasing authority. If the information is designated confidential and therefore not released, the researcher has the right to have the decision tried. First, one should turn to the handling archive officer. Thereafter, the city archivist makes a formal decision with a justification. Appeals are made to the Swedish administrative court of appeals, which is the highest authority. Patient journals more than 70 years old are not considered confidential and are therefore accessible for everyone.

When doing research in medicine, social science or in behavioural sciences, the Public Access to Information and Secrecy Act states that information regarding personal matters as a ground rule shall be regarded as confidential. Moreover, this rule has been extended generally to teaching and researching institutions for all studies in medicine and social and behavorial sciences (7 § offentlighets- och sekretessförordningen, SFS 2009:641). There is also a secondary confidentiality when a researcher receives confidential data; the confidentiality so to speak follows the data. In general, statistical work falls under the law. Finally, there is a particular statute on confidentiality for scientific chronicles of linguistic and ethnological customs. All these rules are applicable on public research, not private."

Official and public documents in Sweden

Raw data needs to be available for other researchers' review. According to the principle of public access to official records, research organisation's actions often are official when secrecy does not apply (Chapter 2, 3§ of the Freedom of the Press Act). But since confidentiality regulations may apply, a document that is public ("allmän") is not automatically an official ("offentlig") document.

"Public document" applies not only to paper but also to "description in writing or pictures as well as film etc." (Press Law). As described by CODEX about the Personal Data Act [4]: "All research at universities – on-going or finished – must follow the statutes on public access to official documents. This means that material used in on-going research – journals, answers to questionnaires, laboratory test answers, notes of oral answers, etc. – are official documents. These laws are in place for the interests of, e.g., funding organisations, patients and society, as regards control of and possibility for inspection. Problems may arise when researchers promise full confidentiality, the application of which is not without problem. Patients and participants in research should be informed about the actual protection of their data and the limitations of those measures. See further a pm from the National Agency for Higher Education, Integritetskänsligt forskningsmaterial, and a report from SUHF: Övergripande principer för offentlighet och sekretess i integritetskänslig forskning.

After an appeal to the Central Ethics Review Board (CEPN) in 2004, the Board opposed a regional board and approved of a project for which the regional board had demanded that secrecy be promised to participants in order for an approval being given. Instead information to participants should include: "Your answers and the results of the study will be kept so that no unauthorized persons can access them". CEPN's decision makes a precedent (Dnr Ö 5-2004). Among those that might get authorized, we find reviewers for journals or scrutinizers at doctoral disputations, those investigating possible fraud in research, and other scientists that want to use the material in their own research. A guide for how to handle the sharing of data while keeping standards of confidentiality has been proposed in the article 'Preparing raw clinical data for publication: guidance for journal editors, authors, and peer reviewers'.
USA & International

In research done in collaboration with US researchers, a question of Certificates of Confidentiality might come up. These certificates are intended to help meet the obligations of confidentiality by preventing forced disclosure of identifiable data during legal proceedings. They are authorized by federal law and granted the U.S. Department of Health and Human Services for information that, if disclosed, "could have adverse consequences or damage subjects' financial standing, employability, insurability, or reputation." The current federal law states that with a Certificate, "persons engaged in biomedical, behavioral, clinical, or other research … may not be compelled in any Federal, State, or local civil, criminal, administrative, legislative, or other proceedings to identify such individuals.""

International guidelines regarding personal information

The OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the Council of Europe's Convention for the protection of individuals with regard to automatic processing of personal data are regarded as the first important international guidelines regarding personal information. These two documents were rather similar and both grounded in the idea of "fair information practices". The Convention is more narrow in content (only ADP, or automatic data processing), and is binding only for the states that have ratified it (as opposed to the Guidelines). Further, OECD has published Guidelines on Security of Information Systems. Also, the UN's Guidelines Concerning Computerized Personal Data Files should be mentioned.

Personal data and privacy are severely compromised, when economic interests and

protection against terror increasingly are used as excuses for exceptions. The Madrid Privacy Declaration demands more stringent protections.

5.3 What does the European laws and regulations mean?

The Data Protection Directive, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of the individuals with regards to the processing of personal data and on the free movement of such data [7], regulates, as mentioned above, the processing of personal data within the European Union. The primary purpose is to protect fundamental rights and freedoms of natural persons (not legal persons or entities such as companies or societies). These natural persons are often referred to as data subjects. The directive also has the purpose to allow free movement of data within the European Union in order that the internal market might prosper.

The data protection duties controls what the data controller, the person who decides of the data gathering and processing. Often the data controller is the person who has legal and tax liability for the organisation. As described in the report Legally eHealth. Putting eHealth in its European Legal Context [8], the main duties of a person controlling personal data includes:

"The data must be collected for specified, explicit, and legitimate purposes. This principle requires that, prior to processing personal data, the controller has to define clearly and precisely the purpose(s) for which the data are to be processed. Moreover, the processing should be transparent. The data controller will, therefore, have to provide the relevant national data supervisory authority and the data subject with certain information regarding the processing, and may only process the data for the purposes for which it was collected.
Thus, a doctor who may share patient identifiable data with another doctor for the purposes of treating the patient may share that same information with another healthcare professional for the purpose of conducting medical research if that purpose originally was given as one of the final uses of the data. It also would apply if this is compatible with the latter (especially if the data subject has given his or her consent to the communication) or if appropriate safeguards are met for processing personal data for medical research viewed as a scientific purpose (i.e., reasonable steps are taken to hide the true identity of a data subject). If the personal data are anonymised by the doctor, there is no problem to communicate the anonymous data to a third party for scientific purposes, including medical research safe for other special rules in National Law (i.e., medical secrecy). Also, they must be processed fairly and lawfully so that if a researcher collects data in order to carry out a specified research project, he or she may not collect and process other data that are not necessary for that particular study but might be useful at some later date. The controller also must ensure the data are kept up-to-date while they are needed, and not kept longer than necessary."

The report Legally eHealth. Putting eHealth in its European Legal Context [8] presents several fictional case vignettes, which outlines the way data protection laws might be applied. Two of them are reproduced below:

Case vignette 1: Second medical opinion from a colleague in another EU contry

" Wilhelm Wolfgang, 50, a building construction manager from Stuttgart, has suffered from

multiple allergies both respiratory and dermatological, since he began working on construction projects at age 18. Other than the recurrent allergies, Wilhelm, a non-smoker, generally has been in good health.

Unfortunately, his most recent routine X-ray revealed some suspicious areas on the upper right lung. Wilhelm's specialist, Dr. Willy Weiss, would like to ask a second opinion regarding the images and the case. He identified Prof. Alexander Artemis, a world expert of pulmonary imaging in the detection of rare lung diseases, located in Greece.

Dr. Weiss wonders whether the digital X-ray images can be transferred safely and securely to Prof. Artemis. A conversation with Prof. Artemis reassures him on that score. In addition, Prof. Artemis is quite happy to provide his analysis free of charge.

Wilhelm is hoping that Prof. Artemis can provide his opinion from a distance, although he is willing to fly over, if expenses can be reimbursed. Wilhelm thinks that two opinions give more credibility to the decisions that will follow."

When analysing the case, the data is found to have been ***lawfully collected*** since the patient has agreed to the X-ray and to its transmission to Greece. Dr Weiss will be subject to the special rules concerning processing of sensitive data. Further, it is ***legitimate to process the medical data*** since Dr Weiss process the data as a registered medical practitioner and it is needed to collect and process the data in order to determine the medical diagnosis. ***The data*** could ***be sent to another country*** since Dr Artemis is a medical doctor in a country in the European Union, and the data is sent in order to make a diagnosis. It is, however, Dr Weiss that has the legal duty to ensure that Prof. Artemis and his hospital provide sufficient security measures.
What are the legal duty of a third-party data recipient? Prof. Artemis is processing the data on behalf of Dr Weiss and must act only on instructions of Dr Weiss.

Case vignette 2: Processing of medical records outside the EU
Dr. Caroline Carrington is a general practitioner who recently arrived in a busy group practice, in Loch Harlow, Lannockshire, Scotland. Dr. Carrington replaced Dr. Charles Cramer, who retired in May 2006, inheriting his carefully handwritten records.

Dr. Carrington wanted to switch to digital records as quickly as possible, before multiplying her own additions to the files.

Dr. Carrington's problem on how to digitalise Dr. Cramer's files seemed to find a providential answer when she opened an envelope from Soft Support Ltd, multinational software specialists. Inside there was a prospectus indicating that International Medical Records Coordinators (IMRC) Ltd., a division of Soft Support, would be stopping in Loch Harlow over the summer to provide record scanning services.

Founded by Dr. Gautam Gandhi, a practicing physician in the UK, IMRC had been sold to Soft Support in 2005. IMRC's business was based on Dr Gandhi's connections between the UK and India. IMRC scans patient records in a mobile unit stationed outside British practices, and then sends them to IMRC offices in India for data entry to populate a database held in the practice. Dr. Carrington wonders if she can make use of the offer of IMRC Ltd.

Is it legally acceptable to digitize paper records? Is such processing of the patient's medical data compatible and necessary with the initial purpose for which the data was collected? Yes, since this would allow Dr Carrington to treat her patients more efficiently. ***Can digitization of paper records be outsourced domestically?*** IMRC would act as data processor, whereas Dr Carrington will have to ensure that IMRC can provide sufficient guaranties on technical and organisational security measures. ***Can further processing be outsourced to outside the EU?*** After scanning the records, IMRC intend to send the digitised files to India (outside EU) to build a database. The transfer of data can only be permitted if India provides an adequate level of protection, which does not seem to be the case. The report Legally eHealth states that: "Such transfer of data to India would be permitted either on the basis of the unambiguous consent from the patient or on the basis of a contract signed between Dr. Carrington and the recipient of the personal data, imposing on the latter the conditions of the data processing based on the standard contract terms available from the European Commission The recipients of the communication have to be subject to confidentiality rules equivalent to those incumbent to health care professionals. Again, to ensure a fair data processing, Dr. Carrington or the practice should inform the patients that the digitalized medical records have been sent to India to be encoded for a database located in the UK."

The rights of the data subject, often patients, are described by the directive (95/46/EC). According the laws in EU countries, the data subject should have access to data stored, and also has the right to ask for correction if the data stored is inaccurate or incomplete. Most European countries have legalisation that allows patients to access their medical records. Further, some data can be regarded as especially sensitive. Legally eHealth. Putting eHealth in its European Legal Context [2] explains that:

"Data concerning a person’s health, religion, trade union activity, as well as data revealing racial or ethnic origin and judicial information, are amongst the data regarded by the Directive as especially sensitive and, therefore, subject to special rules. For this reason, data that are capable, by their nature, of infringing fundamental freedoms or privacy of the data subject normally should not be processed. The ban on processing sensitive or medical data aims to ensure the fundamental rights and freedoms of the data subject regarding the processing of his or her medical data. The ban is, of course, not absolute, so all EU countries hold, by principle, that medical data may be collected or processed only for certain purposes and following certain guidelines, including notably:

- That the explicit informed consent of the data subject is obtained
- To protect the vital interest of the data subject or of another person when the data subject is physically or legally incapable of giving consent
- For the purposes of preventive medicine, medical diagnosis, the provision of care or treatment, or the management of healthcare services, if the data are processed by a health professional subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy."

The report Legally eHealth. Putting eHealth in its European Legal Context provides an overview of legal sources on data protection, and on product and services, which is also provided below [8].

Legal sources on data protection

- **Directive 95/46/CE** of the European Parliament and of the Council of 25 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data
- **Directive 2002/58/CE** of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector
- **Directive 2006/24/CE** of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks. Amending Directive 2002/58/EC
- **Regulation (EC) No. 45/2001** on the protection of individuals with regard to the processing of personal data by the Community, institutions, and bodies, and on the free movement of such data
- **European Convention on Human Rights**
- **Charter of fundamental rights of the European Union**
- **The Convention n°108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data**, adopted on 28 January 1981
- **Convention n°164** for the protection of Human Rights and dignity of the human being with regard to the application of biology and medicine: Convention on Human Rights and Biomedicine and its Additional Protocols
- **Recommendation (97) 5** of the Committee of Ministers to Member States on the protection of medical data, adopted on 13 February 1997
- **Recommendation (83) 10** of the Committee of Ministers on the protection of personal data used for scientific research and statistics, adopted on 23 September 1983
- **Recommendation (97) 18** of the Committee of Ministers of Members States concerning the protection of personal data collected and processed for statistical purposes, adopted on 30 September 1997
- **Recommendation (99) 5** of the Committee of Ministers of Members States for the protection of privacy on the Internet, adopted on 23 February 1999
- **Communication 2004 (356)** from the Commission to the Council, the European Parliament, the European economic and social committee, and the committee of the regions, "eHealth - Making Healthcare Better for European Citizens: An Action Plan for a European eHealth Area"
- **Some opinions or recommendations** made by the Data Protection Working Party
- **Opinion n°13 (1999**) of the European Group on ethics in science and new technologies on ethical issues of healthcare in the information society

Legal sources on products and services liability

Leg*al Sources Concerning Information Society*

- **Directive 1999/93/EC** on a Community framework for electronic signatures
- **Directive 2000/31/EC** of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

Legal Sources Concerning Business and Consumer Protection

- **Directive 2005/29/EC** of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market (Unfair Commercial Practices Directive). This Directive replaces the business-to-consumer rules in the misleading and comparative advertising Directives (Directive 84/450/EEC of 10 September 1984 relating to the approximation of the laws, regulations and administrative provisions of the Member States concerning misleading advertising as modified by Directive 97/55/EC of European Parliament and of the Council of 6 October 1997 concerning misleading advertising so as to include comparative advertising). Those two Directives still apply to business-to-business activities.
- **Directive 97/7/EC** on the protection of consumers in respect of distance contracts
- **Directive 1999/44/EC** of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees
- **Directive 2001/95/EC** of the European Parliament and of the Council of 3 December 2001 on general product safety
- **European Convention on products liability** in regard to personal injury and death of
- **Council Directive 85/374/EEC** of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products as modified by Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999 amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products
- **RoHS Directive 2002/95/EC** of the European Parliament and of the Council of 27 January 2003 on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

Legal Sources Concerning Healthcare

- **Council Directive 90/385/EEC** of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices
- **Directive 98/79/EC** on in vitro diagnostic medical devices
- **Directive 2001/83/EC** of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use
- **Council Directive 93/42/EEC** of 14 June 1993 concerning medical devices

5.4 Privacy and security of data in GiraffPlus

The ethical evaluation for the GiraffPlus project has been considered in Wp6 as it is strictly linked to the establishment and maintain of the test sites. In D6.1 the relevant legislations for the three countries hosting test sites is summarized and the ethical requirements are stated. The Italian legislation requires a free and informed consent from the participant and this will be insured for all participants of the project. In Spain a Research Ethics Committee is tied to the test site where the system will be tested and evaluated. They will ensure the protection of personal data and secure individual rights for involved test persons. The Swedish partner had an ethical

application approved 20/06/2012 by the Regional ethical vetting board in the Uppsala-Örebro region.

The explicit informed consent of the data subject will be obtained for all participants. In Sweden the Data inspection approval of storage of patient data will be required.

5.4.1 Privacy and security requirements

In the GiraffPlus project, we are dealing with personal data, data that sometimes can be very sensitive, both in the sense that it is important that data is not corrupted, and in the sense that personal data must not be revealed to unauthorized persons. Generally in the data dependency and security areas, requirements are divided into the principles *confidentiality*, *integrity*, and *availability*, plus often also *authenticity* and *non-repudiation*. In addition, *legality* has been proposed as an additional principle. We will describe the relevance of each of these principles to data in the GiraffPlus project, and what methods that are suitable to use to ensure privacy and security of the data.

5.4.1.1 Confidentiality

Confidentiality aims at preventing unauthorized access to data. The general ground for confidentiality is that exposing data to unauthorized persons would cause harm or other adverse effects, typically to the proper user or owner of the data.

When dealing with personal data like in the GiraffPlus project, confidentiality is very much linked to *personal integrity*. Monitored physiological as well as environmental parameters can be sensitive to disclosure. A third concern is the disclosure of the collection process itself.

Confidentiality of collected physiological data in the GiraffPlus project

Physiological data, data that is collected to monitor the physical status of a person, of course reveals a lot regarding the physical status of that person. An example can be monitoring of heart activity. A recording of e.g. ECG or heart rate variability can reveal that the monitored person is suffering from a heart condition. Information about this is sensitive, and there can be many reasons not wishing to reveal such a condition, ranging from pure personal privacy (e.g. a person may not wish his or her neighbours to know about the heart condition), to concerns about economic effects (e.g. a person may not wish his or her life insurance company to raise the life insurance premium because of the heart condition).

Confidentiality regarding personal data of this kind is also regulated by law as described above.

Confidentiality of collected environmental data in the GiraffPlus project

Environmental data does not automatically raise the same privacy and legality issues as physiological data. However, in many cases environmental data can be just as sensitive. While information about e.g. the temperature in the kitchen may most often be harmless if revealed to unauthorized persons, other types of information may reveal physical conditions or social activities that the monitored person wishes be kept private. Such simple information as how often and for how long the bathroom is used can reveal sensitive information. Information about the presence or absence of a certain person in a certain room may also be very sensitive.

While confidentiality regarding environmental data is not always regulated by law, the above concerns make it appropriate to treat environmental data the same way as physiological data. It is thus a recommendation that all data receive the same treatment with respect to confidentiality, independent of whether it is physiological data or environmental data.

Confidentiality with respect to the collection process

Sometimes it is not enough to protect data from disclosure. Sometimes the very process of data collection reveals information. From the fact that a data collection is on-going, it is possible to draw some conclusions, e.g. that the monitored person may have a condition that requires monitoring. Hiding that data monitoring goes on can be extremely difficult. Confidentiality should however always be used to conceal the type of data being collected.

For the GiraffPlus project, it can be concluded that the deployment of a Giraff in the home, and the installation of monitoring sensors and communication equipment in the home, will be more revealing than the data traffic itself. It should thus not be a requirement to attempt to hide the communication itself. The type of data should however be concealed from unauthorized access, not only the data values.

5.4.1.2 Integrity

Integrity here means data integrity, i.e. that data cannot be tampered with. Both physiological data and environmental data must be protected from tampering. This includes data en route from sensors to the GiraffPlus middleware, data going from the middleware to the data storage, as well as the stored data itself.

Integrity of data en route

Confidentiality in the form of encryption, together with authentication that the sender is the correct sensor, addresses the integrity problem of data en route. Hence, no special mechanism or method is required for integrity of data en route if confidentiality and authentication is solved.

Integrity of stored data

Data stored in the database must not be tampered with. Cryptographic checksums address this problem. The risk of erasure or unavailability of data stored will be addressed when addressing the availability principle below.

5.4.1.3 Availability

Availability of data means that data should be available to the proper user at the required time. In GiraffPlus, we can again differ between realtime data accessed from the sensors, and data accessed from the data store.

Availability of realtime data

Accessing realtime data means fetching data from sensors, over the networks. This means that the main issue for availability of realtime data is the dependability of the networks. The GiraffPlus system has two types of networks: the wireless sensor network between sensors and middleware, and the network between the middleware and the data storage.

Dependability of the wireless sensor network

The main threat to the wireless sensor network is unavailability due to lack of connectivity between sensor nodes or between sensor nodes and gateway. The source of this lack of connectivity could be intentional or unintentional. In any case, the effect is a lack of connectivity that is hard to remedy. Using redundancy on the link layer can somewhat remedy this problem, but against a full-fledged denial-of-service attack on the wireless sensor network there is really no remedy inside wireless network regulations (prohibiting increasing transmission power significantly) except abandoning the wireless network in favour of a wired network. The risk of such an attack on the wireless sensor network of the GiraffPlus system is however small, and the suggestion is to not try to counter this threat.

Dependability of the network from middleware to data storage

The network from middleware to data storage can be of several types: mobile data, broadband to the home, modem over POTS, etc. Common for all these networks are that the network operator will have taken measures to keep the probability of availability high. However, even these systems do sometimes fail. For an operational system, it should be considered to have redundancy in the connection; with some fall-back should the primary connection fail. For the first GiraffPlus prototype, however, network redundancy could be considered optional.

Availability of stored data

Availability of stored data relies on the network to the data store discussed above. Additionally, the data storage itself should be dependable, meaning that there should ideally be redundant servers geographically separated. For the first GiraffPlus prototype, geographical separation could be considered optional, while server redundancy should be required at least on the level of data being resilient enough to survive disk crashes.

5.4.1.4 Authenticity

Authenticity here means that that it is possible to verify the sender of a particular piece of data, in order to avoid impersonator sensor nodes providing false data, or impersonator servers providing false data. Authenticity is a very important requirement in the face of safety-critical systems, but any system dealing with people should be free from risks that unauthorized entities supply false data to the system.

Authenticity is achieved using some kind of verification process, an authentication. Authentication requires cryptographic mechanisms that guarantee that identities cannot be cloned or forged.

In the GiraffPlus system, sensors can be manually authenticated when connected to the GiraffPlus system.

5.4.1.5 Non-repudiation

Non-repudiation means that the sender of data should not be able to deny sending the data in question. If the sender is authenticated as discussed above, and if the data integrity is guaranteed,

then the non-repudiation problem is solved. There is thus no need for any separate method or mechanism for non-repudiation in the GiraffPlus system.

5.4.2 Methods to insure privacy and security of the data in GiraffPlus

5.4.2.1 Confidentiality

Confidentiality of data en route is solved by using a VPN (Virtual Private Network) connection between the GiraffPlus platform and the server.

Confidentiality of stored data is solved by encryption of the stored data. The decryption key to the encrypted data must be handled in accordance with the regulations described above; only the authorized personnel must have access to the decryption key and thus to the data.

5.4.2.2 Integrity

Integrity for stored data is for hard disks provided by hardware. To avoid data loss in case of disk crashes, redundant disks or a RAID system should be used.

5.4.2.3 Availability

For the first prototype, existing networks and network solutions are sufficient.
For later prototypes, redundant network paths could be considered for increased availability.

5.4.2.4 Authenticity

Authenticity of data en route is solved by the VPN connection between the GiraffPlus system and the server.

Authenticity of stored data is ensured by the encryption of the stored data.
The authenticity of the initial connection of wireless devices to the Giraffplus system is solved manually.

6 Conclusion

This deliverable describes the system with its simple monitoring sensors. It describes also how the sensors are installed at the pilot site. Together with the sensors (the hardware components), the software components deployed in the pilot site are described. The main part of the deliverable is focused on the “gluing” component: the middleware. A detailed description is given for its components, classes and sequence diagrams to allow a complete view of this first prototype of the system and the initial network infrastructure.

The design and development of the overall system by taking into account the functional specifications provided by the WP1 (D1.2, D1.3), and the functional requirements derived by the activities of WP3 and WP4 and feedbacks from WP6 evaluations activities has been coordinated.

All the hardware and software components are currently in place and working in the test apartment and the development of the enhanced and mobile aspect of the middleware is progressing according to plan.

Finally an analysis of security and privacy requirements regarding collecting, processing and transferring of personal information is also presented. Both the European and Swedish legislation are considered as the Swedish legislation in the area can be considered one of the strictest. Two main aspects are considered: the consent and information of the participants in the trials and the security of the data from a technical perspective. How the project is handling them is also outlined.

7 References

[1] http://www.universaal.org

[2] http://www.ibm.com/developerworks/webservices/library/ws-mqtt/index.html

[3] Fielding, Roy T.; Taylor, Richard N. (2002-05), "Principled Design of the Modern Web Architecture" (PDF), ACM Transactions on Internet Technology (TOIT) (New York: Association for Computing Machinery) 2 (2): 115–150

[4] http://cxf.apache.org/

[5] http://httpd.apache.org/

[6] http://developer.android.com/reference/android/os/Binder.html

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of the individuals with regards to the processing of personal data and on the free movement of such data.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[8] Legally eHealth. Putting eHealth in its European Legal Context, Legal and regulatory aspects of eHealth. Study report March 2008, European Commission, Information Society and Media.
http://ec.europa.eu/information_society/activities/health/docs/studies/legally_ehealth/legally-ehealthreport.pdf

[9]"New draft European data protection regime". m law group.
http:/www.mlawgroup.de/news/publications/detail.php?we_objectID=227

[10] Website of CODEX, Centre for Research Ethics & Bioethics, Uppsala, Sweden
http://www.codex.vr.se/en/manniska3.shtml

[11] Personal Data Act - SFS 1998:204
http://www.sweden.gov.se/content/1/c6/01/55/42/b451922d.pdf

[12] Personal Data Ordinance - SFS 1998:1191
http://www.government.se/download/ed5aaf53.pdf?major=1&minor=25633&cn=attachmentPublDuplicator_0_attachment

[13] The Swedish Data Inspection Board's Authority Regulations
http://www.datainspektionen.se/Documents/faktabroschyr-pul-forskning.pdf

[14] Public Access to Information and Secrecy Act Offentlighets- och sekretesslag (2009:400)
http://www.notisum.se/rnp/sls/lag/20090400.htm

[15] Public Access to Information and Secrecy Ordinance Offentlighets- och sekretessförordning (2009:641)
http://www.notisum.se/rnp/sls/lag/20090641.htm

[16] Tryckfrihetsförordning (1949:105)
http://www.notisum.se/rnp/sls/lag/19490105.HTM

[17] The Law regarding health data registers Lag (1998:543) om hälsodataregister
http://www.notisum.se/rnp/sls/lag/19980543.HTM

[18] Patientdatalagen (2008:355) (PDL)
http://www.notisum.se/rnp/sls/lag/20080355.HTM

[19] Nationell Patientöversikt (NPÖ)
http://www.inera.se/Vardtjanster/NPO/

[20] Accompanying regulations on "informationshantering och journalföring i hälso- och sjukvården"
Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14)
http://www.socialstyrelsen.se/sosfs/2008-14