CIP-297225

Deliverable D3.4
Service Migration Guidelines

Kostas Giokas

Due date of deliverable: 31/01/2015

Actual submission date: 06/11/2015

This work is partially funded by EU under the grant of CIP-Pilot actions 297225.

Change History

Version	Date	Status	Author (Partner)	Description
0.1.0	25/06/2015	Draft	Kostas Giokas (SILO)	ToC and draft released
0.1.1	08/07/2015	Draft	Kostas Giokas (SILO)	ToC defined
0.1.2	27/07/2015	Draft	Kostas Giokas	Section 1 Contribution
0.1.3	31/07/2015	Draft	Vincenzo Genovese (SSSA), Sergio Neglia (ENG), Christian Barrue (UPC), Angelo Paolo Castellani (TESAN), Ulysses Cortes (UPC)	Individual Contributions
0.1.4	23/08/2015	Draft	Stephen Hope (DOCOBO)	Individual Contribution
0.1.5	30/10/2015	Draft	Kostas Giokas (SILO)	Section Contribution
0.1.6	05/11/2015	Draft	Kostas Giokas (SILO)	Individual Contribution
0.1.7	06/11/2015	Draft	Stephen Hope (Docobo)	Individual Contribution
0.1.8	06/11/2015	Final	Kostas Giokas (SILO)	

EXECUTIVE SUMMARY

IDF has organized pilots in five countries and the participation of native uses in each pilot site. The multinational and multi-cultural character of the project asks for the localization of the platform in the pilot languages.

This deliverable is the continuation of Deliverable D3.3, which mainly dealt with the localization aspects of the IDF platform in relevance to its migration to the five pre-set pilot sites. In this deliverable, we aim to report on a set of procedures and mechanisms that will enable the migration of the IDF platform in a completely new setting.

This deliverable assumes that all migration issues that are relevant to the localization have been dealt with in Deliverable D3.3 and therefore assumes that these are resolved prior to the platform's new installation.

Finally, the aim of this deliverable is to create a high-level guide for IDF migration that could also be used as a presentation to prospective clients of the IDF platform in order to inform them on the installation/migration procedure.

Document Information

CIP Project Number	297225	**Acronym**	I-DONT-FALL
Full title	Integrated prevention and Detection sOlutioNs Tailored to the population and risk factors associated with FALLs		
Project URL	http://www.I-DONT-FALL.eu		
Document URL			
EU Project officer	Arnaud Senn		

Deliverable	**Number**	D3.4	**Title**	Service Migration Guidelines
Work package	**Number**	3	**Title**	

Date of delivery	**Contractual**	31/01/2015	**Actual**	06/11/2015
Status			final ☑	
Nature	Report ☑ Demonstrator ☐ Other ☐			
Dissemination Level	Public ☑ Consortium ☐			
Abstract (for dissemination)				
Keywords	Fall Detection/Prevention, Architecture, Interoperability, Services			

Authors (Partner)	Kostas Giokas			
Responsible Author	Kostas Giokas		**Email**	kgiokas@singularlogic.eu
	Partner	SILO	**Phone**	+30-210-6266260

TABLE OF CONTENTS

GLOSSARY

IDF	I-DONT-FALL
SSR	Service Specific *Requirements*

1 INTRODUCTION

This document is a very high-level and concise report detailing how to migrate all services for deployment of IDF in a totally new pilot setting. As platform migration also involves localization it is preferable to use Deliverable D3.3 for steps and procedures that are required for the localization aspect.

The main goal of the IDF project is to pilot and evaluate a novel ICT based approach for Integrated Fall Management, which is highly based on the merits of fall detection, fall prevention and fall management integration of technologies and services.

This deliverable aims at supporting the commercialization of the IDF platform after the project's funding period has passed. The scenario for IDF is that due to its pan-European approach (in development and mainly testing and piloting) all partners will have the possibility to suggest new business development should any arise.

This document together with several others (e.g. IDF Localisation, System Manuals, etc) will assist in providing a steady support option for the technical sales personnel of the partner that has found a new customer. Following this document this particular partner will be able to understand the requirements for IDF, prior, during and after its installation in a customer's premises. It has been agreed among the partners that whoever requires assistance in setting up IDF for a new customer the others (IDF subsystem manufacturers/developers) would help in the installation. So for example if new customer in Italy requests for IDF to be installed, Engineering will assume the role of the local technical representative for IDF whereas it will receive additional help from DOCOBO, SiLo, SSSA, UPC and TESAN.

IDF is a complex system integrating a number of technologies very different to each other (developed in a different way) but the past 3 years of close collaboration between the partners has proven to be the most efficient tool for overcoming these diversities. The outcome of this collaboration has been a fully working platform with positive impact to the medical profession (measured in Work Package 7).

2 IDF MIGRATION METHODOLOGY

2.1 Platform Migration Theory and Methodological Approach

While specifics may vary by the technology and business logic involved, migration projects all have many commonalities and can, therefore, be approached with certain common strategies and methodologies. Strategies and methodologies presented in this document are suitable for projects ranging from the smallest data conversion to the largest legacy migration project with a repeatable and systematic approach that ensures predictability and success

A full lifecycle of a migration project are as follows:

- Assessing the current environment to migrate
- Planning for a migration project
- Architecting a new target environment
- Implementing a migration by using available tools and processes
- Managing the newly migrated environment

Focusing on IDF the general “migration” term may not apply in all its sense since migration the movement of technology from older or proprietary systems to newer, more versatile, feature-rich and cost-effective applications and operating systems with the aim to reduce cost and improve interoperability, reliability and manageability. However especially for IDF we will require **infrastructure migration** (e.g. prepare an AREAS server in Engineering ‘s premises then ship it off to the customer) and **application migration**.

Infrastructure Migration

The term *Infrastructure Migration* refers to the process of migrating all layers of the computing platform, not only the applications that support business functionality. This can be a complex exercise that will have a greater impact on the entire IT operations than other strategies would. For example, Infrastructure Migrations can include changes to the following:

- Applications that support business functionality
- Application infrastructure that supports the applications, such as web servers, application servers, middleware and database technology
- Third-party products provided by ISVs
- Application architecture, e.g. multithreading
- Computing and storage platforms, e.g. SAN or attached storage
- Network infrastructure
- Facilities infrastructure, such as power, ventilation and cooling
- Management policies
- System monitoring and management tools
- Locally written scripts to manage applications and data
- Administration and support staff training

Application Migration

The term *Application Migration* applies to applications rather than infrastructures. In particular, it usually applies to custom-written applications and refers to modifying or normalizing the code of an application so it can be recompiled and deployed on a new hardware platform that supports a different Operating System (OS). Application Migration is inherently associated with modifying the code base of an application so that the functionality provided by the Application Programming Interfaces (API) of the existing OS and supporting software products is replicated in the new target environment.

Application Migration typically requires minimal understanding of the logic or functionality of the application. It is a somewhat mechanical effort for making the application compatible with the new environment. An Application Migration strategy requires the integration of the application with a new development environment, as well as with a new operating system. While source code, scripts and data are moved; compilers, source code repositories and software tools are replaced by new versions that are compatible with the target platform.

When migrating an application, any supporting third-party software must also be migrated. If the software is not available on the new platform, similar software must be found and integrated it into the application. Should the amount of integration become excessive, the migration might begin to look less like a re-hosting and more like a re-architecture effort.

A repeatable and systematic methodology for migration that helps ensure predictability and success of migration projects is proposed. IDF should follow a structured architecture methodology built on best practices. Following a structured architecture methodology requires a plan upfront for much of the work that needs to be done. In addition, the application of the methodology ensures collaboration with all of the stakeholders involved in a migration effort to develop an architecture that will address their needs as well as the business objectives.

2.1.1 Migration Phases

2.1.1.1 Assess & Design Phase

The initial assessment and design phase in a migration project addresses the following technical startup-planning tasks for the project:

- Assessing the environment to ensure that all of the assumptions made during project justification have been proved and that all of the requirements and dependencies for the architecture are documented.

The following types of assessment tasks occur during the architect phase:

- Assessing the technologies used
- Assessing processes used
- Assessing people skills needed

· Designing and architecting a migration solution, which includes the following types of tasks:

- Identifying the degree of change required (if this is the case)
- Identifying service level goals

- Documenting design goals
- Creating a component and technique map
- Refining high-level designs
- Creating a transition plan
- Developing a configuration management plan
- Creating a system I/O map
- Creating an acceptance test plan
- Planning test strategies
- Prototyping the process
- Designing a training plan for the new environment

2.1.1.2 *Build and Implement phase*

The build and implement phase of a migration project is the active development of a new environment during which the following types of tasks occur:

- Porting Applications to the new operating system, which includes the following types of tasks:
  - Creating a target build environment
  - Building a new application for the target platform
  - Deciding whether to support backward compatibility
- Migrating data to the new environment by transferring or converting it. This step includes the following types of tasks:
  - Transferring data
  - Transforming data
- Creating the production environment, including the following types of tasks:
  - Building the production facilities environment
  - Building the production platform
  - Building the application infrastructure
- Testing the migrated environment, which includes the following types of tasks:
  - Building the test environment
  - Creating the test plan
  - Performing unit testing
  - Performing regression testing
  - Performing integration testing
  - Testing performance
- Refining the migrated solution
- Training end users and staff

The key deliverables of this phase include working components and documentation. In addition, the implementation phase might possess an iterative structure and might include prototyping. In particular, prototyping is useful for data migration and difficult or risky conversion techniques. The implementation phase can be iterated to allow incremental development. This allows a number of drivers to influence staging. A migration solution may be developed incrementally because different management environments are being migrated in different stages, with training done

before the quality assurance installation; or it could be that the solution's architecture permits a component-based delivery or that the phasing might be based on project or business resource constraints

2.1.1.3 *Manage and Support phase*

The manage and support phase is about sustaining systems and applications at runtime and includes an amount of post go-live, onsite support and mentoring from key members of the IDF post project commercialization team to ensure a smooth hand off and transition and the continued success of the organization in maintaining systems moving forward. Migration is fundamentally an implementation exercise, although the following management tasks are typically within the scope of a migration project:

- Assessing the current IT management infrastructure
- Addressing the critical gaps
- Extending the infrastructure to account for the migration

In some cases, this phase may focus on service delivery and support management to address other issues, including:

- Service level management
- Financial management
- Capacity management
- Availability management
- IT service continuity management
- Service desk
- Incident management
- Problem management
- Change management
- Release management
- Configuration management

Obviously the manage and support stage starts when migrated code is placed into use.

2.2 Pre-Requisites for IDF Migration

2.2.1 Environmental pre-requisites

WIMU

The IP (Ingress Protection) of the WIMU is IP31.

Therefore, the environmental pre-requisites related to the WIMU are that to avoid workspaces in which are present solid objects fewer than 2.5 mm or direct spray of water.

iWalker

The physical training with the i-Walker requires a location with enough room to perform the exercises. Also to perform the assessment tests (e.g. 10MWT or 6MWT) a corridor longer than 10 meters is preferred. It is desirable that the floor surface is not very slippery, so the i-Walker does not present odometry slippage

problems. It is recommended to have a place to park the i-Walker close to a wall power plug

AREAS

Physical access requirements are not considered since AREAS is a software module and resides on a server

SOCIABLE

Cognitive training can be performed indoor in the institutions or in home environment. No particular environmental prerequisites are required (Please also see D2.2)

Careportal

CAREPORTAL is a medical device with an IP rating to IP20 and operating temperatures +4 to 40°C. In general use the surface of the device can be wiped cleaned with 'bio-tissues'. In general use the device should be plugged into a mains source at all times to ensure batteries are charged. When in use it should be positioned out of direct sunlight in a vented situation to prevent overheating by radiated energy.

DST

The Decision Support Tool is a software application that runs via a secure web browser. There are no specific environmental prerequisites for this component of the I-DONT-FALL platform

2.2.2 Technical pre-requisites

SOCIABLE

IDF Sociable runs on a normal PC or a touchscreen device. Below are listed the hardware that could be used to install the IDF-Sociable application:

1. A normal PC running windows Software. In that case there is a loss of functionality in terms of using touchscreen interfaces.
2. A multi-touch monitor (either on tablet, laptop or desktop computers)
3. A surface table providing multi-touch screen functionality.

The multi-touch devices should be compatible with the technical specifications as described in D3.2 SOCIABLE Platform Specification [1]. In particular, the surface laptop hardware had to be selected among the hundreds of surface computer that are available in the market. In order to meet the SOCIABLE requirements, the PC system should comply with the following specifications:

- Large Screen (>15")
- Large resolution
- Easy to use and handle
- Powerful processor
- Windows Vista or Windows 7 environment (in order to alleviate the need for rewriting the cognitive games and other applications for the surface PC environment)

- Multi-Touch functionality, as a key to achieving an ergonomic and motivating environment for cognitive training.

More information on SOCIABLE requirements is available in D2.2

2.2.2.1 *Security*

WIMU

The only requirements of security for the WIMU (for both version: fall detector and logger) are related to the re-charge procedure. Both the wearable and the mobile devices must be re-charged by connecting them to the USB charger when the user does not wear them

iWalker

Wireless network security configuration needs to be provided beforehand in order to setup the i-Walker properly specially in environments with highly restrictive accesses (i.e. hospitals). In cases where the wi-fi configuration is conventional, the user himself can configure it. It is recommended not to use a public Wireless network to connect the i-Walker since the data captured could be exposed

AREAS

Protocol https is chosen to guarantee connections security. It consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security or its predecessor, Secure Sockets Layer

TESAN

Web services interactions are encrypted using Transport Layer Security technology. For this reason, a proper certificate for the host offering these services would be required

SOCIABLE

There are no security requirements for SOCIABLE

Careportal

The CAREPORTAL is a Class IIA approved medical device which meets the information governance requirements in respect of encryption of captured data for onward transmission to the central Docobo Doc@Home DST. However, the data from the iWalker is transmitted to the CarePortal via the WiFi network as described above with due regard to the safeguards noted and the ports of the WiFi router must be configurable to allow this local data transfer

All patient data is encrypted prior to transmission. Information is maintained and stored in CAREPORTAL until it receives a notification from the server that all data has been received and is successfully assigned to the DST database. Only then is the data cleared from memory. Up to a thousand patient data sets can be stored per device. Only the patient data sets that have been transferred successfully are then cleared from the system. No data is lost at any time.

DST

The Decision Support Tool is a secure web browser that accesses the IDF clinical database stored a secure server governed by EU regulatory requirements for data protection and information governance. Access to patient record is on a need-to-know basis and is controlled by individual user names and personalised passwords. Patient data outside of authorised use is anonymized and can be identified to the components of the IDF platform by randomly generated agreement numbers ensuring patient anonymity at all times.

2.2.2.2 *Accessibility*

WIMU

The steps to make the WIMU (for both version: fall detector and logger) working are:

1. wear the WIMU
2. switch on the WIMU;
3. run the FallDetector/Logger app on the Smartphone.

The accessibility of the system can be compared to that of the Smartphone

iWalker

The i-Walker handlebars need to be adjusted to an adequate height depending on the user

SOCIABLE

In order for the elderly to use the SOCIABLE cognitive training system, they should be able to interact with the SOCIABLE applications. A typical example to be employed in games involves pictures, images, puzzles and pieces that should be selected and resized in the context of a cognitive training exercise. In particular, elderly users should be able to:

- touch objects and push them around (like in the real world), but at the same time:
- scale objects by using a two-finger gesture (unlike the real world).

Careportal

For this project the CAREPORTAL is used by both the end-user directly in a home environment and also by the Clinician as a means of controlling the set up of the iWalker and the collection of Data from both the iWalker and WIMU.

Docobo has carried out considerable research prior to this project into Usability and Accessibility issues for its end user deployment particularly with the elderly and those with co-morbidities. Questions can be spoken for those with a visual impairment and on the Standard Careportal which also supports an ECG functionality all the functions can be reproduced by buttons allowing for the equipment to be used by patients with say with Parkinsons Disease with a tremor or neurological conditions that make the use of a touch screen

particularly difficult. The CAREPORTAL is initially set up and individualized for each patient by the clinician who registers a patient on the CAREPORTAL® through the use of an associated agreement number automatically generated at patient enrolment. This is to ensure security Each CAREPORTAL can be set up for individual or multipatient use. In multi patient mode a unique PIN number is generated and notified independently to each patient. When starting a session and interaction between CAREPORTAL and the patient takes place.

Entering the Pin number will bring up a personalised welcome screen for the patient and request confirmation that the patient is the patient indicated on the screen. On confirmation, data can be entered. If the data entry session is not completed the patient is notified that data is still required and is prompted to complete data entry. At the end of an active session, the data is automatically transferred to the server.

DST

Access to the clinical screen of the DST is via a secure web browser and entry of a user name and password. This will allow the clinician to see only the patient data related to the patients assigned to the clinician

2.3 Service Specific Requirements

2.3.1 AREAS EHR

AREAS is the Engineering's Electronic Health Record (EHR) solution customized for the IDF project purposes.

It is a web based solution that can be easily used by a webkit based browser.

To access to this application a username/password binomial is needed and can be provided by administrator with right credential for the user (doctors, nurses, psychologists, caregivers, and so on

2.3.2 DST

The IDF DST hosts the Electronic Health Record created via AREAS and forming part of the record is the Patient data associated with the various tests carried out using the WIMU and i-Walker and the records associated with the Falls Diary that is captured via the CarePortal. The two systems are connected through the Doc@Home B2B interface and patients can be accessed and created through both AREAS and the DST as appropriate. The Patient data from both AREAS such as results from say a Tinetti Test and the DST such as the data collected from the iWalker can be presented on the Clinicians Portal for decision making purposes. This visualization is a key feature of the system.

The technical implementation requirements, especially in respect of resilience and scalability are discussed in detail in Section 3.1.2. However, in respect of the local implementation due regard has to be given to the capabilities of the Clinicians Terminal to access the Clinicians Portal which is an internet connected web browser based application capable of running on a range of computers (desktop computers, laptops and tablet computers).

2.3.2.1 *Basic Requirement Specification for the Clinician Terminal*

- *Browsers Type:* Internet Explorer 8 and above (IE8+), FireFox, Chrome and Safari are supported.
- *Minimum Screen Resolution*: 1024 x 768
- *Screen Size:* The application will run on Tablets and Laptops with sufficient Screen Resolution. However, for readability 17" terminal or larger is preferred
- *Network Connection*: EXTERNAL INTERNATIONAL INTERNET CONNECTION Required
- *Physical Connection:* Wired Connection is preferred over WiFi for assured performance and increased availability.

2.3.2.2 *Security Requirements:*

- The clinician terminals connect to web servers within the clinical system that require a secure connection to be supported (the https protocol).
- Data Encryption will be supported - digital security certificates with key sizes of at least 256 bits.
    - Users require external email address and access to email account
    - For access to the patient data by the clinician the appropriate login information as described for AREAS is required. Role based levels of access can be set up according to local requirements

2.3.3 SOCIABLE

IDF-SOCIABLE is a series of gaming exercises performed using a Microsoft Surface Table. The IDF-SOCIABLE service does not have any specific requirements since it is offered pre-installed and pre-configured with the hardware.

2.4 Post Installation Requirements

2.4.1 Good performance levels

WIMU

The max charging time of the WIMU battery is about 8 hours.

The WIMU Fall Detector is fully working up to 16 consecutive hours.

The WIMU Logger is fully working up to 3 consecutive hours.

In both case the battery life ensures good levels of performances:

1. the re-charge of the Fall Detector must be executed once a day;
2. the re-charge of the Logger must take place after running the six-minute walking test for 10 consecutive patients.

i-Walker

The i-Walker performs a calibration process each time that is turned on that takes approximately 1 minute. In order to perform a good calibration, the i-

Walker needs to be in a flat surface and nobody must be touching it so the sensors calibrate properly.

It is recommended to turn off the i-Walker when the training is over (i.e., not leaving it turned on for days with nobody using it).

Moreover, it is recommended to perform the data transmission protocol with the Careportal to Docobo servers at least once per week in order to speed up the transfer process

AREAS

Sometimes, in very rare occasions, a reboot of the Oracle session can be necessary after some intervention in Docobo's server; it can be done by remote administrator and take not more than a couple of minutes.

SOCIABLE

The Surface Table is in fact a PC-like configuration running Windows OS so it behaves like one (it should require an occasional reboot) so minor performance levels should be dealt with either internally by the IT department or by calling SILO's technical support.

Careportal

CAREPORTAL automatically connects to the server using WiFi, GPRS, 3G and POTS and Ethernet, depending on the actual version deployed and the customer requirements. The device should be positioned close to or within range of the appropriate communication channel. On screen indicators identify communications status. Where cellular communication is used Roaming SIM cards are available which will enable the strongest network to be detected over which to upload patient data and download software updates as appropriate.

For resilience Data can be accumulated (up to 1000 patient sessions) if communication services are disrupted thus ensuring that data is safeguarded

DST

The decision support tool server is maintained and data security checked on a daily basis. All data is backed up daily and encrypted and taken offsite to ensure complete data security. A support team is available on a daily basis to respond to any questions or concerns.

2.4.2 Remote Support

i-Walker

Provided that network is available, remote support can be performed in the i-Walker units in order to assess possible malfunctions. It is recommended the presence of a support person in site in order to help in the diagnostic process. Skype conference calls are used to communicate with the UPC support. The i-Walker includes a Virtual Private Network service that allows the technical staff to connect directly to the i-Walker in a safe and secure way

AREAS

Any intervention to manage AREAS can be done remotely, except for the case of hardware failure

SOCIABLE

Microsoft Surface table can be remotely operated as a normal PC provided it is connected to a public IP address. All software aspects of SOCIABLE can be dealt with remotely. However, most hardware failures should be dealt with, via Microsoft Hardware support. SILO will be responsible for contacting (in coordination with the client) local Microsoft Hardware service providers.

CAREPORTAL

Questions sets and other administrative data are downloaded to the equipment as required are downloaded remotely to the CAREPORTAL during the time at which the equipment is connected to the server for the upload of data.

DST

Upgrades and maintenance on the DST server are carried out during scheduled periods where customers are given advance warning of such work

2.5 Good practices, updates and security

i-Walker

The i-Walker should be charged after each use. If the batteries remain empty for long periods may lead to a malfunction.

The i-Walker charger is a delicate device; it must be unplugged pulling the plug head and never pulling the cord. Pulling the cable leads to a charger malfunction.

The i-Walker should be charged while turned off. It is recommended that the i-Walker is unplugged from the charger before turning it on. Some isolates cases have been detected where not doing so could lead into a malfunction of the i-Walker unit.

The i-Walker has two informative lights on handlebars that inform users about its state. It is highly recommended to contact the support staff if it presents non-conventional flash behaviors. Normal behaviors are described in the manual.

If needed the i-Walker unit can be diagnosed and updated remotely if and only if network connection is provided. If the unit needs hardware repairs it should be sent back to the producer for repairing.

CAREPORTAL

CAREPORTAL® should be placed onto its cradle, when not being used to enter data, making sure that it is properly seated in its place. If the mains socket has a switch, it should be turned to the ‘on’ position. When first used allow for 15 minutes to ensure the battery has adequate charge the monitor is ready for use. Always return CAREPORTAL® to is cradle immediately after use.

The screen of CAREPORTAL® provides indication of the operational status of the device. On the left hand side of the upper information area a signal strength

indicator is displayed if connected by 3G or broadband otherwise a WiFi icon will be displayed. If there is no connectivity this will be indicated in this area.

The position of CAREPORTAL® should be such that an adequate WiFi connection is maintained. If connected directly via ethernet this not necessary.

CAREPORTAL software and applications are automatically updated on connection to the Decision Support Tool (DST) server. Each monitor has a password accessible extended settings function whereby the current software, communication and operational status of the device can be checked.

All data is secured by 256-bit encryption at the point of data entry. After enrolment there is no personal identified information is displayed except for the session welcome message with associated prompt message: Good Morning Mr First Name / Last name, Your next questions and tests are due now! To start answering questions press OK.

DST

The Decision Support Tool receives the information entered by patients and structures the data in a meaningful format for assessment by clinicians. The IDF interface on the DST allows for the set up and structuring of the clinical displays and the decision support interfaces.

Only authorised clinicians can access the system by use of an exclusive user name and personal password. All patient/end user data is presented in a structured format and organized by sub departments of the clinical organisation thus enabling patients to be viewed only by their own clinician or clinicians given authorised use. The DST has achieved the highest level information governance in its country of origin (NHS Information Governance Toolbox) and is subject to continuous security evaluation and assessment year on year.

All data is reported in accordance with the local organization's information governance guidelines. Server software is updated and maintained and all changes and use is logged

Encrypted data can be exported to approve servers such as the prospective client's electronic healthcare record, typically demonstrated by I-DONT-FALL's AREAS operating system.

2.5.1 Bug fixing and support

IDF project strategy to support users is done by the unique email contact point support.IDF@eng.it

The technical support team take in charge the request and it is sorted to the owner of the bug/malfunction. In this way the shortcut between user and technician is created and the dialogue start for eventually further clarifications needed to solve the issue.

Each owner of single device/application (Docobo, Engineering, SSSA, UPC, TESAN) has proper strategy for preventive maintenance (bug fixing)

2.5.2 Security (Physical & non-physical)

Physical security should be taken care by the customer, all devices that can be removed should be locked away. Data security is an issue but it is again up to each customer to abide to their respective security plan (e.g. firewall access, etc.)

2.5.3 Overall Good practices – Lessons Learnt (LL)

Please refer to deliverable D7.8 where the IDF overall good practices are presented in more detail.

3 IDF SERVICE AND PLATFORM SPECIFIC MIGRATION

3.1 IDF Service Specific Migration [silo]

3.1.1 AREAS Migration

AREAS doesn't need any software distribution since it is a web application accessible throw a webkit based browser as minimum requirement.

When the Server owner has set correct access credentials to the dedicated physical spaces and has given the url to reach the application (e.g.: https://id1.docobo.net) the application is ready to be used by the authorized users.

If the authorized user can reach the application with the right credentials, it means that any link is well designed and deployed.

Another test to verify the connection with Docobo server is the use of DST button that (if all works properly) open another window with the Docobo User interface aiming to access *i*-Walker and WIMU data

3.1.2 Careportal Migration

The IDF system provided by Docobo comprises two elements; the CarePortal, and the Decision Support Tool (DST)

Careportal

The CarePortal is an Android based Care Platform which is a fully commercial offering and deployed across many thousands of patients across Europe and beyond. It operates with a customised version of the DocoboApp for the IDF Project and is used for the control and capture of data from the i-Walker and WIMU, and also provides other services such as the Falls diary and other physiological and symptomatic condition data which are standard features as required by the clinician.

From a service migration perspective, the DocoboApp itself can be used on a number of Android devices including the purpose built CarePortal, which has an ECG feature and is itself a Class IIa Medical Device, A tablet style device and a mobile phone. In these cases, the DocoboApp is a Class I Medical Device. Screen readability for the intended user is a key aspect in the choice of such devices. In addition, in order to maintain the memory requirements and other operating system requirements such as security the devices should not be upgraded to new versions of Android without specific reference to the manufacturer Docobo, who will check compatibility before a new release is delivered to the device over the Air.

From a specific Service Migration perspective, the CarePortal Units are normally purchased by the customer from Docobo or their partner with the specific software build for the application preinstalled and tested by Docobo.

Decision Support Tool (DST)

Approach to Service Migration

The DST is based upon the well-established Docobo Doc@Home Telehealth System which itself is a Class I Medical device and is approved for the storage and management of Medical Data. Docobo already offer different approaches to service migration

a) Running a remote system centralised on our Doc@Home Server and buying just the CarePortals. This is an option frequently adopted by our National Health Service customers, as our system is N3 approved which means it is directly linked to the secure health service network. This is regarded as a lower cost option as it is then not necessary to make an investment for the servers and maintain a secure IT system

b) Export an instance of the Doc@Home Application to other customer servers and as long as they follow the instructions that we provide then the medical device status can be maintained as would be that of Careportals that would be purchased and attached to the new implementation. This is similar to the way that people will buy a blood pressure machine. There is a licensing agreement for this arrangement. However a key factor would be the compliance by the organisation with and maintenance of Local Information Governance requirements and suitable quality systems in place to support this deployment

Scalability

To facilitate scalability the server should be hosted in a virtualised server farm as indicated in Figure 1 The key components here are

- Virtual server hardware, in pairs, configured to provide high availability failover redundancy.
- Network attached RAID storage providing operating system and data storage for servers, they're being two of these to provide failover redundancy.
- Managed switches in a high availability, dual redundant pair, these having multiple redundant connections to the servers and network attached storage devices.
- Firewalls in a high availability, dual redundant pair.

The virtual servers should be provisioned with at least 16 cores and 64 MB RAM, and should be provisioned for enterprise use with quad gigabit networking and dual power supplies, as should the network attached storage devices.

In terms of application support, the servers in the farm should be a combination of Windows 2012R2 servers for telehealth interactive use and device connectivity OS, and Ubuntu 12.04.5 LTS for database and AREAS hosting.

Simpler configurations could be considered, for example a 2 server cluster, and this would suffice for a small or satellite installation, but would lack scope for capacity scaling.

Regarding installation, the virtualised infrastructure indicated in Figure 1 would require custom / bespoke set up. Operating system and basic application software installation would use installers. However, specific server provisioning would require custom / bespoke set up.

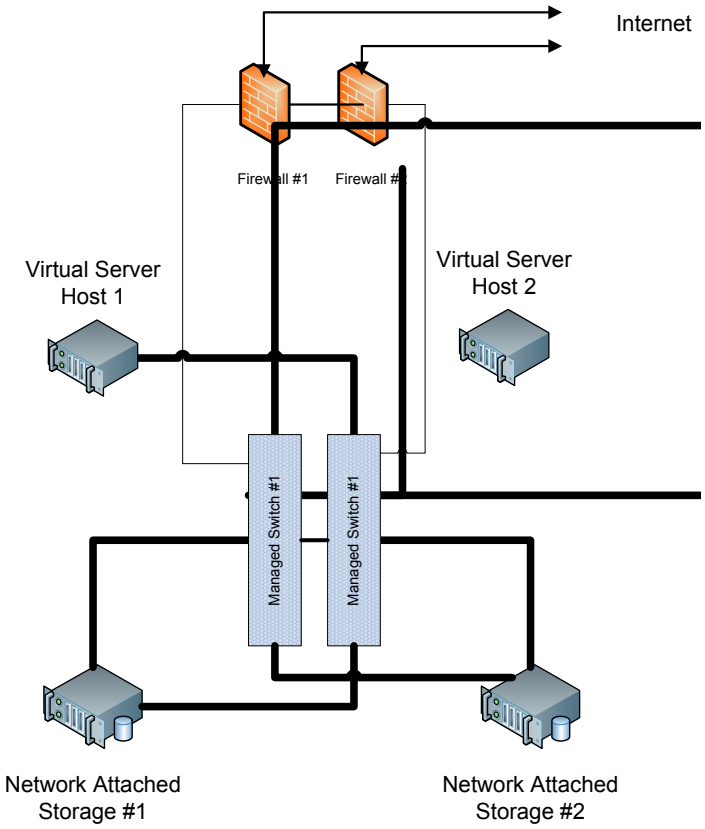

Figure 1 - Server installation

Internationalisation and Localisation

In respect of internationalisation and localisation Docobo has developed a translation engine that enables translations of the appropriate text done by translators for the CarePortal and Clinicians Portal to be structured in such a way that the right language can be presented for the various Clinician Windows and CarePortal programmes. (including Greek)

As Doc@Home and CarePortal are medical devices a key point of the localisation aspect of the service migration in respect of this is that the translations for the devices are clinically validated should they be implemented by third parties

3.1.3 SOCIABLE Migration

SOCIABLE comes pre-installed with Microsoft Table. SILO is an authorized Microsoft Table reseller with offices in many EU countries with Microsoft's presence. If a client is outside these countries, SILO's engineers will setup

SOCIABLE according to the setup procedure described in the relevant document [Installation Manual for IDONTFALL – SOCIABLE 2] that accompanies this deliverable.

3.2 Platform Integration Approach

[*in this section, we require input that is similar to the previous paragraph but more appropriate for WIMU, iWalkse and TESAN. The input should be more focused on delivery of the hardware, its assembly, first charge, etc. Also the integration with the rest of the platform is of the essence]*

3.2.1 WIMU Integration

The WIMU, has been designed and developed in two versions, respectively:

1. Fall detector, to face of the problem of fall detection in elderly people;
2. Data logger, to allow the logging of inertial data related to the dynamics of the human body.

When the WIMU is delivered there is no need to execute any assembling.

The device must be charged before the first usage by means of a USB charger.

A red led on the device is switched off when the charge has been completed.

In both versions the WIMU needs a connection to a mobile device (an Android Smartphone) hosting a specific application capable to acquire via Bluetooth the data/alerts collected/generated by the wearable device and to extend these results via WiFi or mobile to the rest of the IDONTFALL platform.

Therefore, the first step of the WIMU integration is related to a connectivity issue to be faced on the Smartphone:

1. the WIMU Fall detector must have the Smartphone working on Internet (via WiFi and/or mobile);
2. the WIMU logger must have the Smartphone connected to the same WiFi network to which is connected to the Careportal.

In the case of the Fall Detector, the service related to the generated alarm is based on the web service technology. The WIMU generates an alarm, the alarm is sent to the mobile device and hence it is propagated to the Call Center by invoking a web service. Therefore, the only requirement for a correct migration of the Fall Detection service is that to have a Call Center capable to handle this technology. The coordinates of the Call Center (URL, user name, password, web service name) must be reported in the file CCENTERinfo.txt stored on the Smartphone under the directory ../IDONTFALL (see WIMU User Manual).

In the case of the Data Logger the related service doesn't involve the presence of any remote system. The data collected by the WIMU are sent to the mobile device which in turn sends them subsequently to the Careportal via WiFi by using the ftp protocol. The adopted protocol allows to the Careportal and the Smartphone to find automatically their IP addresses. Therefore, the data logger doesn't present any migration issue.

3.2.2 iWalker Integration

- A courier service delivers the the i-Walker unit on-site, with a USB unit with the manual and network configuration files.
- The USB contains a video explaining *how* to assemble the i-Walker unit and *how* to start using it.
- After network configuration, integration with the IDF platform is complete; Careportal can access it.

3.2.3 TESAN integration

TESAN ICT system have been tightly interfaced with the IDF platform, so that as soon as a new patient joins the experimentation, directly through the platform an enrollment form containing the information required by the TESAN service center is compiled.

As soon as the validity of the information inserted in the IDF platform have been verified by the operative staff, a unique alarm ID token is assigned to the patient.

Through this procedure the TESAN call center is then integrated out-of-the-box with any WIMU or i-Walker device, since as soon as they are correctly binded with the intended patient using the alarm ID token, TESAN can handle any alarm generated by these devices

SOCIABLE

The details for integrating SOCIABLE with IDF can be found in D4.3 I-DON'T-FALL Integrated Platform Final Version

Careportal

CAREPORTAL is a class is a medical device that uses the Android operating system. Applications and services (i.e. SOCIABLE) can be integrated with CAREPORTAL and the (range of CAREPORTAL products) to allow patient use.

Devices running Microsoft operating systems can run the DocoboAPP programmes which replicate the functionality of CAREPORTAL to fully integrate SOCIABLE applications

Data transfer to CAREPORTAL can be achieved through USB, WiFi or direct Ethernet connection. This data is then configured for transfer to the DST via the standard communication process

DST

The DST is a web based application based on the Docobo Doc@Home product. An instance of the Doc@Home Application can be exported to other customer servers and instructions for integration are provided to customers to ensure that the medical device status can be maintained

However, a key factor would be the compliance by the organisation with, and maintenance of Local Information Governance requirements and suitable quality systems in place to support this deployment

AREAS

More on the AREAS integration can be found in deliverable D4.3 I-DON'T-FALL Integrated Platform Final Version

4 PLATFORM MIGRATION BEST PRACTICES AND PITFALLS

4.1 Conclusions from current installations

From a DST implementation perspective experience has shown with the current IDF configuration that split server and DB is not efficient. However, for resilience it is anticipated that there would be a master database and a replicated hot standby. Scalability also has to be considered in this respect.

From a SOCIABLE implementation perspective there are no major issues. The Microsoft Surface Table is bulky and heavy and not easy to move around so physical installation should be thought off in advance. Windows OS is preloaded and preconfigured and no updates (Windows Update or other) should be run unless approved by SILO.

5 CONCLUSIONS

In this deliverable we have tried to produce guidelines for the successful pre-installation, installation and post-installation procedures of the IDF platform. We have identified those prerequisites that would make IDF's installation easier from the respective partners, commented on the use of the equipment and informed the reader on what is to be expected after the initial use (and subsequent thereof) of the system.

We have provided a methodology that allows the potential customer to accommodate the IDF platform in the easiest way possible and well as given instructions of good use (not as detailed as in the manuals) of IDF's subsystems.

Although IDF is a complex platform to install as it requires the integration of many technologies, the IDF project has proven that at least in the six pilots, the IDF platform has been installed and has run successfully for the duration of the pilot study.

This deliverable can be viewed as a prelude to the scalability feasibility of the IDF project and can be used in conjunction with deliverables D3.3 Services Migration, Localization and Customization Specifications and D8.5 Sustainability Plan. This deliverable is logically followed by D2.2 Fall-Detection-Prevention Functionalities and Operative Protocols

Related documentation:

D3.1 Detailed Technical Specification of Fall Detection and Prevention Services

D3.2 I-DON'T-FALL Integrated Platform Architecture and Technical Specifications

D3.3 Services Migration, Localization and Customization Specifications