COMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME

ICT PSP call for proposals 2008 - ICT PSP/2008/1

Project Acronym:	**Long Lasting Memories**
Project Number:	**238904**
Project Type:	**Pilot Type B**
Project Full Title:	**Long Lasting Memories**

ICT PSP Main Theme addressed: **1.4: ICT for ageing well with cognitive problems, combining assistive and independent living technologies**

D6.3 National and European Security and Certification Requirements Including Issues of Liability

Nature:	Report
Dissemination Level:	Public
Version #:	1.40
Delivery Date:	29th July 2010
Deliverable Leader:	ATHENA R. C.
Author(s):	Eleni Vlahou, Nadia Economou
Status:	Final
Reviewed on	28th July 2010
Reviewed by:	Cryssa Sardeli (AUTH)

Abstract

Report on National & European Security and Certification Requirements & Issues of Liability, in order to provide the necessary background on specific security issues and certification procedures that must be addressed for the successful market deployment of the LLM service and its compliance with international and European security policies and standards.

Document History

Version	Issue Date	Stage	Content and changes
#1.0	23 June 2010	Draft	Initial version, in outline form, issued to project partners for comment and preliminary input
#1.1	12 July 2010	Draft	Revised version based on input from partners EIKON and Tero
#1.2	16 July 2010	Draft	Input from all partners is included
#1.3	23 July 2010	Prefinal	Draft document ready for internal review
#1.4	28 July 2010	Final	Reviewed by AUTH

List of participants:

1	ARISTOTELIO PANEPISTIMIO THESSALONIKIS / Medical School	AUTH	Greece
2	UNIVERSITAT KONSTANZ	UKON	Germany
3	ATHENA RESEARCH AND INNOVATION CENTER IN INFORMATION COMMUNICATION & KNOWLEDGE TECHNOLOGIES/ Institute for Language and Speech Processing	ATHENA RC	Greece
4	Tero Ltd	Tero	Greece
5	CEIT RALTEC gemeinnuetzige GmbH	RALTEC	Austria
6	INVESTIGACION Y DESARROLLO INFORMATICO EIKON SL	EIKON	Spain
7	Fundacion INTRAS	INTRAS	Spain
8	E-SENIORS: INITIATION DES SENIORS AUX NTIC ASSOCIATION	E-SENIORS	France
9	GLOBAL SECURITY INTELLIGENCE LIMITED	GSI	UK
10	GENIKO NOSOKOMEIO ATHINAS IPPOKRATEIO / Health Centre Vyronas	IGNA	Greece
11	Milton Keynes Council	MKC	UK
12	Municipality of Schwechat	SW	Autria
13	National and Kapodistrian University of Athens	NKUA	Greece
14	University of Cyprus	UCY	Cyprus

Executive Summary

The purpose of this Report on National & European Security and Certification Requirements & Issues of Liability is to provide to the LLM consortium the necessary background on specific security issues and certification procedures that must be addressed for the successful market deployment of the LLM service and its compliance with international and European security policies and standards.

This deliverable is organized in three sections:

In the first section, international, European and national standards for information security requirements are examined. As far as national requirements are concerned, standards are covered for all the countries involved in the consortium.

In the second section, software specification requirements are introduced, covering both European certification and national certification standards for all the countries involved in the consortium.

Finally, in the third section issues or interoperability and liability are dealt. The integration schema introduced by the LLM system is fully described; based on these requirements, third party applications can be designed and developed to allow consistent cooperation with the LLM system. Concerning liability, policies deriving from the ISO 27001 protocol are expanded to cover issues concerning the LLM project.

The regulations and documents which are discussed in the present deliverable may serve as directly applicable to the LLM service, or as advisory in nature.

Table of Contents

1 INTRODUCTION

1.1 Why Standards Are Important

Alzheimer's Disease (AD), often preluded by Mild Cognitive Impairment (MCI), has been characterized as one of the most debilitating and costly diseases internationally (Alzheimer's Association, 2009). Specifically, a Delphi Consensus Study regarding the prevalence of dementia worldwide (Ferri et al., 2005) revealed that more than 4.6 million elderly individuals are diagnosed with dementia every year (i.e. a new case of dementia is diagnosed every 7 seconds), and that this number will double every 20 years. Even more dramatically, these numbers are expected to increase by 100% until 2040 in all the developed countries. Regarding countries of the European Union, 10.8 million elderly people (i.e. over the age of 60) are expected to have been diagnosed with dementia by 2020, a number that will increase and reach up to 15.9 million diagnosed dementia cases by 2040. Additionally, the healthcare costs of the EU countries rise faster than the economic growth of these countries, according to the "ICT for Health, Ageing and Accessibility" report of Comyn for the European Commission. These statistics clearly stress the need for the design and dissemination of a cost-effective intervention which will prevent, instead of treat, many MCI or even healthy cases of elderly people from converting to AD or other forms of dementia.

Since the current health-system models seem to inadequately cover the need for preventing dementia in a cost-effective manner, the way a medical practitioner's knowledge is applied for such a purpose to elderly individuals must change. In this line, according to Comyn, the healthcare systems must change from hospital-based to home-based. That is, this preventive intervention must enable people to use it at home, thus must be portable and user-friendly, especially in the case of elderly users many of which are expected to be unfamiliar with ICT services and products. What is more, interoperability must be another characteristic of such a solution, since it will lower its cost and advance its usability by the elderly.

During the last years, healthcare products and services have been rapidly developed leading to a great variety of innovative applications. Modern healthcare solutions offer personalized services, integrate communication devices and process information related with the participant's health status. However, medical information is regarded as highly sensitive. Therefore, development of healthcare services should be regulated by special security standards.

As we enter the 21st century, software has become a critical part of our businesses, our products, and our daily working environment. Anytime software fails, businesses incur losses through lost worker productivity, lost revenue, lost potential sales, lost customers, lost or corrupted data, and expenses necessary to bring systems back up, and to recover and reconstitute data. In spite of the overwhelming dependence on software, businesses today have little basis on which to judge the quality of software in order to make informed software procurement decisions. Currently, businesses rely on the reputation of the software vendor, software vendor marketing, anecdotal evidence from colleagues, and published software reviews in order to decide which software applications to buy. Even published reviews rarely deal with the quality of the software, nor can they since they do not have adequate time or resources to test the software.

Establishing national, European and international standards security and other regulatory standards enable organizations to practice safe security techniques to minimize the number of successful security attacks. The compliance with these standards should be the strategic decision of any organization, especially if it includes obtaining certification and security insurance.

The adoption of a unified standardization procedure is expected to create new market opportunities through technological innovation. International standardization reduces both the cost of development and maintenance, since it facilitates the adoption of open architecture and interoperability. Products that are conformed to the requirements posed by the standards are greatly favored by the consumers. Industry competiveness is enhanced through the feasibility of products' comparison, while small or new coming industries get protected from monopoly effects. Moreover, the market's unification level, which is a prerequisite towards effective co-operation, is enhanced. Broadly accepted standards offer complete, reliable and efficient solutions, since they incorporate mature technological solutions resulted from many years of research. Therefore, developers have not to spend numerous resources attempting to incorporate research results from the scratch.

Security standards have been created recently because sensitive information is now frequently stored on computers that are attached to the internet. Also many tasks that were once done by hand are carried out by computer; therefore there is a need for Information Assurance (IA) and security. Cyber security is important to individuals because they need to guard against identity theft. Businesses also have a need for this security so as to protect their trade secrets, proprietary information, and customer's personal information. The government also has the need to secure their information.

2 SECURITY REQUIREMENTS

2.1 European Security Requirements

2.1.1 ISO/IEC 27001

ISO/IEC 27001 is an International Standard, published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS) within the context of the organization's overall business risks and specifies requirements for the implementation of security controls customized to the needs of individual organizations. The requirements set out in this International Standard are applicable to all organizations (e.g. commercial enterprises, government agencies etc), regardless of type, size and nature 1,2. More specifically, some of the requirements in this International Standard include:

- understanding an organization’s information security requirements and the need to establish directions and principles for action with regard to information security and a risk assessment methodology[1]
- implementing and operating controls, identify the appropriate actions, resources, responsibilities and priorities for managing information security risks in the context of the organization’s overall business risks
- monitoring and reviewing the performance and effectiveness of the ISMS, detect errors, identify attempted and successful security breaches and incidents and whether the actions taken to resolve a breach of security were effective
- taking appropriate corrective and preventive actions and aiming at continual improvement based on objective measurement.

An ISMS may be certified compliant with ISO/IEC 27001 by a number of Accredited Registrars worldwide. Certification against any of the recognized national variants of ISO/IEC 27001 by an accredited certification body is functionally equivalent to certification against ISO/IEC 27001 itself[2].

The certification process usually involves (a) an initial, preliminary review of the ISMS (e.g. checking the existence and completeness of key documentations such as the Risk Treatment Plan etc), (b) a detailed and formal audit, where the ISMS is tested against the requirements specified in ISO/IEC 27001 and, if it passes this stage, is being certified as compliant with this International Standard and (c), a follow-up audit to confirm that the ISMS remains in compliance with this International Standard[3].

2.1.2 The Common Criteria (CC)

The Common Criteria (CC) – ISO/IEC 15408 – Evaluation Criteria for Information Technology Security are considered the international standard for information technology (IT)

[1] Examples of risk assessment methodologies are discussed in ISO/IEC TR 13335-3, Information technology — Guidelines for the management of IT Security- Techniques for the management of IT Security

[2] http://en.wikipedia.org/wiki/ISO/IEC_27001

[3] http://en.wikipedia.org/wiki/ISO/IEC_27001

security and provide a complete methodology, notation, and syntax for specifying security requirements, designing a security architecture, and verifying the security integrity of a product, system, or network. Roles and responsibilities for a variety of stakeholders are defined, such as customers (corporations, government agencies, and other organizations who wish to acquire security products, systems, and networks), developers (system integrators and vendors who sell commercial security products) and evaluators (accredited Common Criteria Testing Laboratories, which perform an independent evaluation of the security integrity of a product, system, or network)[4].

This International Standard represents the outcome of series of efforts to develop criteria for an IT security evaluation methodology which will assure that the specification, implementation and evaluation of appropriate security standards have been conducted in a rigorous and standard manner.

In the Common Criteria documentation[5]:

- In Part 1 - Introduction and General Model, general concepts and principles of IT security evaluation are defined and a general evaluation model is presented[6,7].
- Part 2 - Security Functional Requirements, includes a catalogue of functional components that will meet the common security functionality requirements of many IT products, organized into classes, families, and components[8].
- Part 3 - Security assurance components defines the evaluation criteria and the assurance requirements of the CC. It includes the EALS[9] that define a scale for measuring assurance for TOEs[10,11].

Common criteria evaluations verify the target's security features through the following:

- Protection Profile (PP): a document which identifies security requirements for a class of security devices. Product vendors can choose to implement products that comply with one or more PPs, and have their products evaluated against those PPs. In such a case, a PP may serve as a template for the product's ST (Security Target, see below), or the authors of the ST will at least ensure that all requirements in relevant PPs also appear in the target's ST document[12,13].

[4] D. S. Herrmann (2003). Using The Common Criteria for IT Security Evaluation

[5] http://www.commoncriteriaportal.org/thecc.html

[6] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and General Model, url: http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R1.pdf

[7] The Common Criteria ISO/IEC 15408 - The Insight, Some Thoughts, Questions and Issues, url: http://www.sans.org/reading_room/whitepapers/standards/common-criteria-iso-iec-15408-insight-thoughts-questions-issues_545

[8] Criteria for Information Technology Security Evaluation - Part 2: Security Functional Components, url: http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R3.pdf

[9] "Evaluation Assurance Level", the numerical rating describing the depth and rigor of an evaluation. Each EAL corresponds to a package of security assurance requirements which covers the complete development of a product, with a given level of strictness. Common Criteria lists seven levels, with EAL 1 being the most basic (and therefore cheapest to implement and evaluate) and EAL 7 being the most stringent (and most expensive).

[10] "Target of Evaluation", defined in "Criteria for Information Technology Security Evaluation - Part 1: Introduction and General Model" as a "…set of software, firmware and/or hardware possibly accompanied by guidance"

[11] Common Criteria for Information Technology Security Evaluation - Part 3, url: http://www.commoncriteriaportal.org/thecc.html

[12] http://en.wikipedia.org/wiki/Common_Criteria#Issues

[13] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and General Model

- Security Target is the document that identifies the security *properties* of the target of evaluation. It may refer to one or more PPs. The TOE is evaluated against the security functional requirements which are established in its ST. In general an ST describes requirements for a TOE and is written by the developer of that TOE, while a PP describes the general requirements for a TOE type (e.g. firewalls)[14,15].

2.2 National Security Requirements

2.2.1 Austria

The Austrian pilot partner RALTEC is performing its IT work based on the principles of ISO/IEC 27001 (as decribed in chaper 2.1.1).One special demand of ISO/IEC 27001 is protection of private data during all SW-processes. This issue is regulated by law the Federal Act concerning the Protection of Personal Data (Datenschutzgesetz 2000 – DSG 2000)

In Austria, the right to data protection and privacy is a fundamental right, as stated in the Federal Act concerning the Protection of Personal Data, passed in 1999 to ensure that Austria complied with Directive 95/46/EC. This act has been in force since 1 January 2000. Details are described in LLM document D6.2.

This law demands registration of each entity dealing with personal date at the national data protection board (“Datenverarbeitungsregeister). RALTEC has applied for registration.

Certification is done in Austria by “Qualityaustri” (/www.qualityaustria.com)

The Common Criteria (CC) – ISO/IEC 15408 – Evaluation Criteria for Information Technology Security is applied in Austria, although there are no certifications done by an Austrian body, Austria has singed the Common Criteria Mutual Recognition Agreement, where Austria is represented by the CIO of the Federal Chancellor’s department.

No certifications are issued in Austria, although certificates issued by a “*Certificate Authorizing Participant*” are valid.

2.2.2 Cyprus

In Cyprus the body that is responsible for any medical research or projects is the Cyprus national Bioethics Committee (http://www.bioethics.gov.cy/Law/cnbc/cnbc.nsf/DMLindex_en/DMLindex_en?OpenDocument). Anything related to the above is subject to be approval from this committee. In accordance with article 3 (1) of the Law N. 150 (I) /2001 The Bioethics (Establishment and Function of the National Committee), the Committee’s mission is the constant monitoring, survey, systematic analysis and evaluation of the issues and problems that relate to the scientific research, progress and implementation of the sciences of biotechnology, biology, medicine, genetics and pharmaceutics as well as to the human intervention on the biological procedure and the human genotype and the investigation of their moral, deontological, social,

[14] http://en.wikipedia.org/wiki/Common_Criteria#Issues

[15] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and General Model

humanistic and legal dimensions. The Cyprus National Bioethics Committee (CNBC) was established in 2001 by the Law No. 150 (I) of 2001, Law Providing for the Establishment and Function of the National Bioethics Committee. The CNBC is an independent body and is not subject to the administrative control of any ministry, independent officer, department or service and has the powers provided by the present or any other Law.

The CNBC has 13 members, including the chairperson. The members represent different professions and disciplines, and are appointed by the Council of Ministers of the Republic of Cyprus for a term of office of four years. According to the provisions of the legislation, at least four members must emerge from the humanities and social sciences sector; four members must emerge from the area of medical and biological sciences, and four members from the area of any other science or profession or who are distinguished in any area of activity for their contribution.

The law files under which CNBC is functioning can be found online at: http://www.bioethics.gov.cy/Law/cnbc/cnbc.nsf/All/538006E398361B89C22571C9002B25A1?OpenDocument. Any application forms of the committee can be found at: http://www.bioethics.gov.cy/Law/cnbc/cnbc.nsf/DMLapplform_en/DMLapplform_en?OpenDocument.

Also there is a private company, the **CYPRUS ORGANISATION FOR STANDARDISATION (CYS)** which is the standardization company in Cyprus.

The CYS is the national organization for standardization of Cyprus. The CYS functions as Company of Private Right with only shareholder the state, managed from 7 members Board of directors. Constituted from representatives of Ministries of Finance and Ministry of commerce, Industry and Tourism as well as institutions of private sector as the Contact of Consumers, the OEV, the KEVE, the ETEK. The CYS is complete member of international organizations for standardization ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). Also the CYS functions as the national centre of standardization and represents Cyprus in the European organization for standardization CEN, CENELEC and ETSI. The CYS participates actively in the international and European standardization promoting the national interests, while at the same time promotes the application the European and international standards in the Cyprus enterprises.

Sectors

Electrical - Electronic Engineering	Heating, Cooling & Ventilation
Health Care	Gas
Health & Safety	Mechanical Engineering
Household Goods, Sports and Leisure	Transport & Packaging
Chemicals & Environment	Services
Food & Biotechnology	Building & Civil

	Engineering
Information Technology & Telecommunications	

CYPRUS ORGANISATION FOR STANDARDISATION (CYS)
30 Kosta Anaxagorou & Lemesou Av., 3rd Floor, CY-2014 Nicosia
P.O.Box 16197, CY-2086 Nicosia
Tel: +357 22 411 411, Fax: +357 22 411 511
E-mail : cystandards@cys.org.cy

LIBRARY OF STANDARDS
Tel: +357 22 411 413, Fax: +357 22 411 433
E-mail : library@cys.org.cy

2.2.3 France

Proposed unique national electronic identity / France [eID ; eSignature]

The present French government has, attached to the Prime Minister, a Secrétaire d'État chargée de la prospective et du développement de l'économie numérique, this can be translated into State Secretary in charge of the prospective and development of digital economy. The State Secretary has launched a unique national electronic identity number programme, called IdéNum, aiming at identifying and authenticating digital services users; this project has some similarity with OpenId (<http://openid.net/foundation>) but remains national, as opposed to global. The first IdéNum prototype is expected end 2010. This "unique national electronic identity number" would be different, separate, from the national social security number, or from the national identity card number, it is assumed.

Schematically, this IdéNum label would allow its users to access on-line services with just one and only digital certificate, thus cutting on repetitive certification and other identification procedures (via SMSs, securised CDs, password generators, etc.). The certificate could be stored on a ciphered USB key, or a SIM card (for using with a mobile phone linked to a computer eg.) and used every time it is needed. It would be a "physically portable" certificate.

France is quite late in this respect, as Austria, Estonia, Finland, Italy, Norway, Slovenia Sweden and Turkey, have already implemented such portable digital certificates for their citizens.

Again, a comparable approach is available, but only on-line as opposed to "physically portable", from the OpenId Foundation.

International standards on electronic signature can be seen at: <http://www.afnor.org/profils/activite/tic/signature-electronique>

2.2.4 Germany

VDE Mark for appliances as technical equipment according to the Appliance Safety Law (GSG), for Medical Device Law (MPG), components and installation materials. The VDE Mark indicates conformity with the VDE standards or European or internationally harmonized standards resp. and confirms compliance with protective requirements of the applicable EC Directive(s). The VDE Mark is a symbol for electrical, mechanical, thermal, toxic, radiological and other hazards.

2.2.5 Greece

The development, promotion and implementation of standardization in Greece is the primary objective of the Hellenic Organization for Standardization (ELOT)[16], which was established in 1976 as a non-profit legal entity under private law, subsidized by the State and supervised by the Minister of Industry.

Activities of the Organization include the elaboration and dissemination of standards, the granting of conformity marks and certificates to products, the certification of management systems, the execution of laboratory tests and inspections.

More specifically, according to Law 372/76 “Establishment and Operation of ELOT”, as amended by Law 1682/1997 and Presidential Decree 155/1997 “ Incorporation and Statutes of the Societe Anonyme ‘ Hellenic Organization for Standardization S.A’”, ELOT has been entrusted with the development of Certification activities. According to Ministerial Decision 22792/509/26-6-1998 “Certification Procedures of the Hellenic Organization for Standardization S.A”, issued by the Ministry of Development (Government Gazette 708/B/13-7-98), ELOT applies Certification Procedures and Systems (e.g.: ISO certification systems).

In the context of these Procedures, ELOT grants Conformity Marks and Certificates of Conformity, which denote the conformity of products, processes, activities, organizations, systems and personnel to the requirements of normative documents. These are called ELOT Hellenic Conformity Marks/ Certificates and are awarded exclusively by ELOT.

In order to respond to market needs, ELOT has developed and operates a scheme for the certification of Information Security Management Systems, according to the requirements of standard BS 7799 and ISO/IEC 27001-2005[17]. The certification process involves the following steps[18,19]:

- The enterprise submits an application to ELOT and all necessary documentation that is requested.
- An inspection team is constituted or, in case of rejection of the application, ELOT informs the enterprise stating the reasons of the rejection.
- ELOT performs an initial, informal inspection (e.g. checking the existence and completeness of key documentation such as the organization's information security policy). Through this step the auditors and the organization are familiarized with each other.
- ELOT performs a detailed and formal compliance audit, testing the ISMS against the requirements specified in ISO/IEC 27001. The auditors will seek evidence to confirm that the system has been properly designed and implemented. Passing this stage results in the ISMS being certified as effective, reliable and compliant with ISO/IEC 27001.

[16] http://www.iso.org/iso/about/iso_members/iso_member_body.htm?member_id=1759

[17] General Regulation for the Assessment and Certification of Information Security Systems, url: https://sales.elot.gr/quality/sadpgr.pdf

[18] General Regulation for the Assessment and Certification of Information Security Systems, url: https://sales.elot.gr/quality/sadpgr.pdf

[19] http://en.wikipedia.org/wiki/ISO/IEC_27001

- ELOT continues to conduct follow-up inspections on a yearly basis, in order to ensure that the organization operates as specified and intended.

Contact:
Hellenic Organization for Standardization
313, Acharnon Street
GR-111 45 Athens
Tel: +30 210 21 20 100
Fax: +30 210 21 20 131
E-mail: info@elot.gr
Web: www.elot.gr/

2.2.6 Spain

All the actions, procedures and services that require authentication by the public administration or citizens by electronic means are processed via the electronic headquarters. The methods for citizen authentication to enable interaction with the administration when secure identification is required are those established by Article 13.2 of Law 11/2007, of 22 June, on Citizens' Electronic Access to Public Services:

- Electronic signature systems included in the Spanish National ID Card for individuals.
- Advanced electronic signature systems, including those based on recognised electronic certificates, accepted by public administrations.
- Other electronic signature systems, such as use of approved codes in a prior user registration, provision of information known by both parties and other non-cryptographic systems, under the terms and conditions determined in each case.

3 SOFTWARE CERTIFICATION REQUIREMENTS

3.1 European Certification Standards

3.1.1 Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens (IDABC)

IDABC (Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens) is a European Union programme managed by the European Commission's Directorate-General for Informatics and established by Decision 2004/387/EC[20]. IDABC aims to identify, support and promote the development of interoperable pan-European e-Government services. It builds on the achievements of the preceding IDA programmes, which focused on improving the effectiveness of telematic[21] information exchanges between public administrations.

IDABC uses the opportunities offered by Information and Communication Technologies to encourage and support the delivery of cross-border public sector services to citizens and enterprises in Europe, to improve efficiency and collaboration between European public administrations and to contribute to making Europe an attractive place to live, work and invest.

To achieve its objectives, it issues recommendations, develops solutions and provides services that enable national and European administrations to communicate electronically while offering modern public services to businesses and citizens in Europe. The programme also provides financing to projects addressing European policy requirements, thus improving cooperation between administrations across Europe[22,23].

The development of pan-European e-Government services takes place through the establishment of networks in Community policy sectors and is supported by measures such as the establishment of portals for businesses and citizens, the provision of technology and software solutions and other support activities[24].

Citizens and enterprises are increasingly benefiting from the various IDABC projects, either by using directly some of the IDABC networks, or by open and efficient public services (e.g. citizens and businesses can refer to SOLVIT, an Alternative Dispute Resolution Mechanism, to help them assert their internal market rights and tackle issues rapidly and pragmatically without having to resort to legal action, etc)[25].

[20] http://ec.europa.eu/idabc/en/document/2560/5849

[21] defined as a "a comprehensive data-communication system, comprising the physical infrastructure and connections as well as the related services and application layers, thus enabling the interchange of information electronically between and within public administrations as well as between public administrations and businesses and citizens;" (DECISION 2004/387/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 21 April 2004 on interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC), url: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_181/l_18120040518en00250035.pdf)

[22] http://en.wikipedia.org/wiki/IDABC

[23] http://ec.europa.eu/idabc/en/chapter/3

[24] http://ec.europa.eu/idabc/en/document/2560/5849

[25] http://ec.europa.eu/idabc/en/document/2586/3

3.1.2 European Union Public Licence (EUPL)

The EUPL is the first European Free/Open Source Software (F/OSS) license. It is consistent with the copyright law in the Member States of the European Union, while retaining compatibility with popular open-source software licenses such as the GNU General Public License. The EUPL is considered a unique legal instrument, as it has been elaborated in respect of European law requirements and has legal value in 22 official languages of the European Union. It can be used for software distribution by European Institutions, national, regional or local administrations, other public entities as well as private entities and natural persons[26,27,28].

The purpose of the EUPL is not to compete with other F/OSS licenses that already exist, but to promote a new wave of public administrations to embrace the Free/Open Source model to valorise their software and knowledge, starting with the European Institutions themselves. That is, the main objective of the European Commission is to distribute widely and promote the use of software owned by itself and other European Institutions under an Free/Open Source Licence conform to European law requirements. The EUPL is compatible with some other copyright licenses, including the GPLv2[29].

3.1.3 IEC 61508

IEC 61508 ("Functional safety of electrical/electronic/programmable electronic safety-related systems") is an international standard of rules which are intended to be applicable to all kinds of industry[30]. It provides functional safety requirements to help a system either work properly or fail in a predictable manner. These requirements can be used for many different types of systems including those with mechanical, electrical, electronic and programmable electronic components. Requirements cover general safety management systems, specific product design requirements and design process requirements[31].

3.1.4 ICT Security Standardisation : ISO/IEC 17799:2005 and ISO/IEC 27001

The most important ICT Security standard is the ISO/IEC 17799 and recently the ISO/IEC 27001. Both standards focus on information security management. ISO/IEC 17799 deals with information security management regarding topics of initiation, implementations and security maintenance. Special attention is attributed to the development and monitoring of an information security policy that covers most aspects of security, including organizational and personnel issues, communication and operations management, access control, etc.

Both standards are based in the following 4-fold model:

- Establishment of security policies, objectives, targets, processes and procedures related with information security and risk analysis.

[26] http://ec.europa.eu/idabc/eupl

[27] http://www.osor.eu/eupl/introduction-to-the-eupl-project

[28] http://en.wikipedia.org/wiki/European_Union_Public_Licence

[29] http://www.osor.eu/eupl/introduction-to-the-eupl-project

[30] http://en.wikipedia.org/wiki/IEC_61508

[31] Foller & Goble. Open IEC 61508 Certification of Products, url: http://www.exida.com/articles/IEc%2061508%20Cerftification.pdf

- Implementation of the aforementioned processes and procedures.
- Monitoring, assessment and report the performance of the processes
- Identify lack of system's performance and take corrective actions in order to improve the security model

Both standards are generic and therefore could be applied in a wide variety of organizations. They are adopted by almost any enterprise that seeks for certification. Their implementation for healthcare solutions should be even stricter due to the special nature of the information need to be stored.

3.1.5 CEN/EN12251: Secure User Identification and Authentication by Passwords-Management and Security

It focuses on the improvement of the authentication of individuals wishing to utilize a healthcare IT system. It strengthens the automatic software procedures associated with the management of user identifiers and passwords, without needing additional hardware facilities.

This standard contains three informative annexes describing guidelines for:

1. Password complexity
2. User responsibilities
3. Password communication

The standard deals with the following issues:

- Unique identification and authentication
- Log-on procedure
- Password storage and logging of passwords
- Password expiration notification
- User-changeability of passwords
- Password reuse
- Password complexity issues

3.1.6 CEN EN14485 (2003) Guidance for handling personal health data in international application in the context of the EU data protection directive

According to the EU Directive on Data Protection, the transfer of personal data from an EU member to a third country that does not ensure an adequate level of protection is prohibited. The specific European standard describes data protection issues that should be govern transmission of personal health data:

- Anonymization
- Definition of the means employed during the transfer of personal health data

- Involvement of data controllers in each country ensuring adequacy of data protection in the context of their own internal organizational rules and their own legal regulatory environment.
- Issues linked with security policy, risk analysis, report of security indents, patient rights, training and awareness

3.1.7 CEN ENV13608 Security for healthcare communication

This standard can be applied to a healthcare communication protocol and information system. It is consisted of the following parts:

1. Concept and terminology Part: It specifies a methodological framework towards the definition, expression and selection of a Communication Protection Profile (CPP) by providing:
    - Standardizing the way of expressing healthcare user security needs in relation to communication
    - Definition of a method dealing with the successive refinement of policy statements used for the identification of standardized security information specifications.
    - Security aspects dealing with the communication protection profile such as integrity, confidentiality, availability and auditability.
2. Securing healthcare objects

It provides guidelines regarding the securing procedures that are implemented in order to facilitate data transfer over open, unsecured networks or their storage in repositories with the same limitations such as the networks. This European Standard is based on existing security standards, without considering how the actual security is applied to the objects. A security infrastructure is assumed, which is used for performing the actual security operations.

3. Security of data channels

It includes the specification of the methods used for enabling the security within the context of healthcare communications. So, data integrity is preserved as well as confidentiality and accountability. A secure data channel is defined as a reliable communication protocol that implements the following security services:

- Authentication of communicating entities prior to the communication of any other data preservation of data integrity;
- Preservation of confidentiality of the communicated data.
- A secure data channel protocol operates in two distinct phases, which, however, may be repeated:
    1) Negotiation phase: authentication of communicating entities (e.g. exchange of certificates), negotiation of the cipher suite to be used, derivation of a shared secret using a key exchange algorithm;
    2) Communication phase: transmission of user data encrypted according to the negotiated cipher suite.

3.1.8 CEN/ENV12924: Security Categorization and Protection for Healthcare Information Systems

The objective of this European standard is two-fold, since it aims at the specification of a method used for the categorization of automated healthcare information systems regarding their security level, while it also specifies for each category a corresponding set of protective requirements adjusted according the category's risk level. The categorization of healthcare products is performed regarding the availability, confidentiality and integrity features of the information that should be administered (communication, processing or storage). The determination of the appropriate category is based according to the values attributed to these features. The standard set of the values given are the following:

1) Availability: Non-critical and Critical.
2) Confidentiality: Non-sensitive, Sensitive and Very Sensitive.
3) Integrity: Non-critical and Critical.

Six out of the twelve possible combinations are selected to form six system categories. The environment in which the HIS operates is also taken into account. This standard defines nine Physical Environment Assumptions, three Physical Connectivity Assumptions and three Logical Connectivity Assumptions. They correspond to the various conditions under which a HIS operates.

For each System Category a corresponding Protection Profile is given. Each Protection Profile consists of Baseline Protection Requirements and Higher Level Protection Requirements. The Baseline Protection Requirements are common to all the Protection Profiles and correspond to the minimum acceptable level of protection. The requirements include Environmental and User Requirements, System Requirements, Contingency Planning, Protection of the Operational Environment, Media and Documentation Control, System Maintenance, Data Exchange and Networking, Software Development, Personnel Measures, Virus Protection Measures, and Compliance with National Legislation.

3.1.9 CEN/ENV12388: Algorithm for Digital Signature Services in Healthcare

This European standard defines the methodology used for creating digital signatures, which role is vital in various healthcare security topics like:

1) Authentication of computer users, organizations and systems
2) Authentication of document originators
3) Document integrity protection
4) Insurance of content and signature binding

3.1.10 ISO/TS 17090 Health Informatics – Public Key Infrastructure

1) Framework & Overview

This part deals with the basic infrastructure contents and outlines the interoperability requirements towards the establishment of a public key infrastructure for secure communication of health related data. Among the topics related with this part of the standard are the identification of the major stakeholders and the main sequrity services that are required. It also provides a brief introduction to public key cryptography, while it also introduces different types of certificates, public key identity certificates and associated attribute certificates, for relying parties, self-signed Certification Authority (CA) certificates, and CA hierarchies and bridging structures.

2) *Certificate profile*

Specification of the certificate profiles required for interchanging healthcare data and deals with digital certificates in health industry.

3) *Policy management of certification authority*

This part gives guidelines for certificate management issues involved in implementing and operating a healthcare PKI. It specifies a structure and minimum requirements for certificate policies, as well as a structure for associated certification practice statements. ISO/TS 17090-3 also identifies the principles needed in a healthcare security policy for cross-border communication and defines the minimum levels of security required, concentrating on aspects unique to healthcare.

3.1.11 ISO/TR 21089:2004 Health informatics –Trusted end-to-end information flows

It offers a guide to trusted end-to-end information flow for health(care) records and to the key trace points and audit events in the electronic entity/act record lifestyle. It also offers offers recommendations regarding the trace/audit detail relevant to each. It offers recommendations of best practice for healthcare providers, health record stewards, software developers and vendors, end users and other stakeholders, including patients.

3.1.12 ISO 22857:2004 Health informatics – Guidelines on data protection to facilitate trans-border flows of personal health information.

It provides guidance on data protection requirements to facilitate the transfer of personal health data across national borders. It does not require the harmonization of existing national standards, legislation or regulations. It is normative only in respect of international exchange of personal health data. However, it may be informative with respect to the protection of health information within national boundaries and provide assistance to national bodies involved in the development and implementation of data protection principles.

3.1.13 DesignForAll

According to a recent report by the Information Society Policy Link (ISPL, 2010), Europe’s population is ageing disproportionally to EU’s birth rates, average life expectancy in European countries is currently over 80 and rising, and by 2020 about ¼ of Europe’s population will be over 65 years old. Hence, the needs of senior citizens become a crucial matter that must be addressed. Additionally, as community health care costs are elevating due to the aforementioned increase in life expectancy, a prerequisite for protecting the EU's public finance sector and the social models of all the EU country-members is to enable senior citizens to remain healthy, independent and productive members of the society.

In the frame of designing an effective ICT solution based on existing technologies, which will aid elderly people to remain active and healthy members of modern societies, it is of vital importance to consider specific ICT standards regarding the population it addresses (i.e. elderly people).

Thus, the needs and the special characteristics of senior citizens who wish to live an independent life must be addressed by such an ICT solution. Importantly only 10% of EU citizens over 65 years of age use the internet (ISPL 2010). This is a clear indication that elderly people are mostly excluded from ICT. Thus special care must be taken to create a user-friendly environment (.g. with a touch screen) which will motivate seniors to use an ICT solution and will be characterized by simplicity (e.g. all the automatic functions of the solution will be controlled via that screen) and efficacy of use.

According to the Ambient Assisted Living Report (AAL, 2006) though, not too many automatic functions should characterize an ICT solution as this creates to the elderly users a feeling of lack of control over the automatic devices and hence estranges them from the very technologies especially built to attract them. Thus automatisms should be restricted to the minimum and most important.

Firstly of vital importance for a person over 60 years of age is the feeling of security their house environment provides them with (van Berlo, 2005). According to the AAL report (AAL 2006) to enhance home security by ICT means, an assisted-living solution must provide an automatic means by which the cooker will be switched off when the user has forgotten to do so (e.g. sensors).

Secondly, care services must be provided. That is, the senior user must be provided with (1) easy and fast access to contacting a medical care service in case of emergency, when remembering and dialing a telephone number will most probably be quite difficult and (2) an alarm which will be automatically activated in case of an emergency via sensors placed in the house, when the person cannot actively contact a care service by herself (e.g. in case the person falls; AAL 2006).

Thirdly, warmth and comfort should be considered: (1) electrical screens on the windows which will be easily handled as well as (2) easy dialing of relatives and friends. Finally, the usability of the cognitive and the physical training components is directly related to its simplicity (i.e. no complex instructions, a user-friendly environment with large and colorful pictures, physical and cognitive exercises resembling a game which will offer visual and verbal reward to the user so he/she is kept motivated to re-do the exercises the next day).

3.1.14 CE Mark

CE stands for Conformité Européenne, "European conformity" in French. Products to be sold in the European Union (EU) that come under certain European Directives must bear the CE mark since it is a legal requirement[32,33,34].

[32] en.wikipedia.org/wiki/CE_mark

CE marking on a product is the manufacturer’s declaration that the product complies with the essential requirements of all the Directives that apply to it. It indicates to the appropriate bodies that the product may be legally offered for sale in their country.

The requirements for CE marking differ across all the Directives and may also vary for different products within a Directive. Depending on the product, CE marking may be as simple as formulating a technical file, or as complex as having to submit your products to regular independent scrutiny.

CE Marking is only required in the European Economic Area (EEA) which includes all 27 member states of the European Union (Austria, Belgium, Bulgaria, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland,, Italy, Latvia, Lithuania, Luxembourg, Malta, The Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom) and three EFTA members, namely Iceland, Liechtenstein and Norway. Although Switzerland is a member of EFTA it is not a member of the EEA.

On the other hand, Turkey is neither a member of the EU nor the EFTA or EEA however, Turkey has implemented many of the European CE marking directives and therefore requires CE Marking for many products.

With the CE Marking being like a passport for the EEA (European Economic Area) it allows manufacturers to freely circulate their products throughout the EEA. Instead of adapting the products for each national market according to the regulations, there now is only one set of requirements and procedures in designing and manufacturing a product within the EEA. For consumers CE Marking has the benefit that products will be safer and therefore damage and liability claims will be reduced.

A list of products that require CE marking is the following:

- Active implantable medical devices
- Cableways
- Construction products
- Electrical equipment
- Electronic equipment
- Equipment and protective systems for use in explosive atmospheres
- Explosives for civil use
- Gas appliances
- In vitro diagnostic medical devices
- Lifts
- Machinery
- Medical devices
- Measuring Equipment
- New hot water boilers
- Non-automatic weighing instruments
- Personal protective equipment
- Pressure equipment
- Radio and Telecommunications terminal equipment
- Recreational craft

[33] www.ce-marking.org/
[34] http://www.cemarking.net/

- Simple pressure vessels
- Toys

The following products do not require CE marking:

- Chemicals
- Cosmetics
- Foodstuffs
- Pharmaceuticals

The procedure for obtaining CE marking is the following:

1. Identify the Directives that are applicable to the product. If more than one applies, the product has to conform with all of them. The directives can be downloaded from the EU website for free[35].
2. Identify the conformity assessment procedure that must be taken. This could either be self-declaration, involve testing inspection or quality system assessment from a Notifies Body or a combination of these.
3. Determine the date by which action must be taken/ the relevant directive comes into force. Most directives are already in force and therefore it is an offence to place products on the market without CE Marking.
4. Identify if there are any Harmonized European Standards applicable to the product. Although some of them are not mandatory for manufacturers, there is a presumption that conformity to these standards will give conformity with the relevant part of the directive
5. Ensure that the product complies with all the essential requirements of the Directives.
6. Identify whether independent assessment of the conformity is required by a Notified Body.
7. Maintain technical documentation required by the directives. This should support your compliance with the directives.
8. Prepare the Declaration of Conformity and the supporting evidence. Along with the technical documentation it should be available to Competent Authorities (EU members) upon request.
9. Check that no other purely national requirements exist in the countries the products are to be sold. (national standards, packaging/ labelling requirements, etc.)
10. Affix the CE Marking to your product and supply user operating instructions.

[35] http://ec.europa.eu/enterprise/policies/european-standards/documents/harmonised-standards-legislation/list-references/

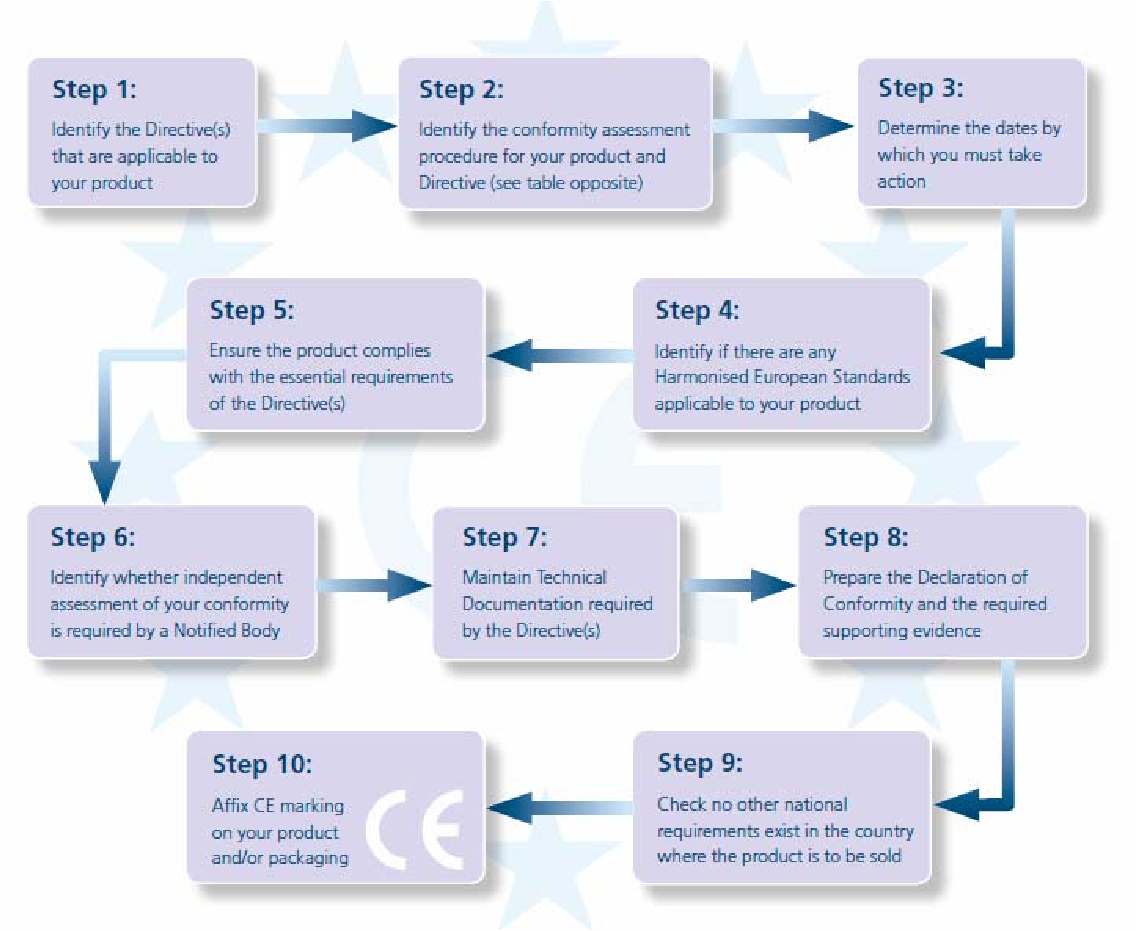
Step 1:
Identify the Directive(s) that are applicable to your product
Step 2:
Identify the conformity assessment procedure for your product and Directive (see table opposite)
Step 3:
Determine the dates by which you must take action
Step 4:
Identify if there are any Harmonised European Standards applicable to your product
Step 5:
Ensure the product complies with the essential requirements of the Directive(s)
Step 6:
Identify whether independent assessment of your conformity is required by a Notified Body
Step 7:
Maintain Technical Documentation required by the Directive(s)
Step 8:
Prepare the Declaration of Conformity and the required supporting evidence
Step 9:
Check no other national requirements exist in the country where the product is to be sold
Step 10:
Affix CE marking on your product and/or packaging
CE

Figure 1: procedure for obtaining CE marking

3.2 National Certification Standards

3.2.1 Austria

Certification of safety-concerning issues of (technical) products and solutions is done by TUeV – technissher Ueberwachungsverein. All kinds of products, processes, services can be certified by TUev.

These certified products, process, solutions get the right to show

The following pictogram “TUeV AUSTRIA”

TÜV also acts as a certification body for products which get certified according the German law of device- and Product safety (deutsches Geraete- und Produktsicherheitsgesetzes - GPSG).

These certified products, process, solutions get the right to show Pictogram "GS"

The department "Trust IT" of TUeV Austria certifies computing centres according ISO27001IT-services, IT-products, IT-applications

TUeV Austria – Technischer Ueberwachungsverein Austria: www.tuev.at

3.2.2 Cyprus

Certification of safety-concerning issues of (technical) products and solutions is done by TÜV Cyprus Ltd. TÜV Cyprus Ltd. was founded in 2006, but has - as a former TÜV HELLAS regional office - been active in Cyprus since 2001. Today, the company is one of the country's largest and most reliable certification organizations.
The service offering of TÜV Cyprus is aimed at both private companies as well as pubic facilities and covers the testing and certification of products, systems, and plants. All legal regulations and directives of the Cypriot and European law are taken into consideration.
TÜV Cyprus has highly qualified employees and works together in close cooperation with strategic partners as well as TÜV HELLAS and other companies of the TÜV NORD Group.

TÜV Cyprus Ltd.
41, Athalassa Av., Strovolos
2012 NICOSIA
Cyprus
Phone +357 22442840
Fax +357 22442850
http://www.tuvhellas.gr/

3.2.3 France

Software certification / France

Certification processes are numerous, often depending on "software manufacturers" or service companies. Most large consulting companies will have their own software qualification methodology.

However, CFTL, Comité Français des Tests Logiciels, the French affiliate to the ISTQB, International Software Testing Qualifications Board, seem to have a more independent approach. CFTL recommend ISTQB syllabuses to companies that organise training courses for qualifying independent « software testers », according to accurate internationally approved syllabuses, freely available on-line (from the ISTQB site). CFTL don't actually directly certify software.

As a certification is needed, it seems the most appropriate step to take to that end is consulting LNE, a certification body described further below, under the "Laboratoire National de Métrologie et d'Essais" title. Interestingly, LNE would be in a position to certify both software and any physical system developed for fitness.

Standards

Like most European countries, France has its own Standards Institute, AFNOR. AFNOR stands for Association Française de NORmalisation. AFNOR are the central operator of the French standardisation system. AFNOR Normalisation's mission is to anticipate standardisation needs and to ensure constant adequation of standards with markets.

AFNOR play a major part within CEN, Comité Européen de Normalisation, which clusters the standardisation institutes of the EU and EFTA/AELE (European Free Trade Association). Three languages are officially used within the CEN, english, german and French. AFNOR are responsible for the French version.

Laboratoire National de Métrologie et d'Essais (also know as LNE, Laboratoire National d'Essais).

Dated 10 January 1978, a law, known as « loi Scrivener » reinforces LNE's missions as regards consumers' protection and information.

LNE are a national reference laboratory for industry (metrology), anticipate new needs in terms of measurement and trials, and assist state and economic players in elaborating new regulations and standards, new trial methods and market surveillance.

Thus, in that framework, they have a "fitness" experience as quoted hereunder:

Fitness

Vélo d'appartement, stepper, tapis roulant, presse de musculation...

Référentiel : normes NF EN 957-1, NF EN 957-2, NF EN 957-4 à 10

Therefore, for this kind of equipment, the standards referred to are: NF EN 957-1, NF EN 957-2, NF EN 957-4 to 10.

[Vélo d'appartement=recumbent bike, Stepper=stepper, Tapis roulant=treadmill, Presse de musculation= press weight].

LNE have a proposal for companies wanting to calibrate systems in several fields, including health care systems. LNE are also an official certification body.

Concerning LLM, it makes sense to assume that all the components (computer, screen, Wii Balance, Blue tooth dongle (if any), Wii mote, e-Home components, etc. taken separately are "approved", On the other hand, LLM as a whole system, requiring increased attention as well as physical efforts from its senior users and, including the collection of personal data, and other product use statistics may require additional certification. The Laboratoire National d'Essais is the body qualified for this certification.

3.2.4 Germany

TÜV

The TÜV (for Technischer Überwachungs-Verein, Technical Inspection Association in English) is a German organization that works to validate the safety of products of all kinds to protect humans and the environment against hazards. They are an independent consultant and examine all sorts of energy installations, devices and products. The TÜV organizations also provide certification for various international standards, such as ISO9001:2008 and ISO/TS16949.

The GS-Mark

The GS-Mark is the German national mark that demonstrates that a product has been tested and found to comply with the standards for the product. The GS-Mark is very well recognised by German consumers; so well recognised that certain products are nearly impossible to sell without the GS-Mark.

For manufacturers and importers wishing to sell their electrical products in Germany, it is a good idea to have a GS-Mark. There are three particular areas where a GS-Mark is nearly a necessity: tools, IT equipment and electromedical equipment. Manufacturers of tools often have a hard, if not impossible, time selling their products in Germany without a GS-Mark because such marking is supported by consumers and the trade unions. IT equipment is also effected by the requirement for GS-Marking; the mark is a requirement if you wish to sell major companies or institutions.

The third area where the GS-Mark is particularly important is electromedicine because a GS-Mark is a prerequisite for a grant to the institution in question from the German authorities.

3.2.5 Greece

The Hellenic Industrial Property Organisation (OBI)[36] is the only legally qualified institution for the protection of inventions and industrial designs in Greece.

As part of its responsibilities, OBI grants the following titles to protect inventions:

1. **Patents**: A Patent is a title of protection valid for 20 years issued to the proprietor for an invention which is new, involves an inventive step and is capable of industrial application. These inventions may either be products, product manufacturing methods or industrial applications.

2. **Patents of Addition (PoA)**: A Patent of addition is a protection title granted for an invention which constitutes a modification to another patent-protected invention (main patent). The PoA follows the fate of the main patent and expires with it. The PoA is only granted to the proprietor of the main patent.

3. **Utility Model Certificates (UMC)**: The Utility Model Certificate (UMC) is a title of protection valid for 7 years issued to the proprietor for three-dimensional objects with a predetermined shape and form which ‘provide a solution to a technical problem’ and have the characteristics that they are 'new' and ‘capable of industrial application’. The UMC may be granted for tools, implements, devices, vessels, components, etc., for example.

In order to obtain a patent, PoA or UMC there is a standard procedure that needs to be followed. This procedure is described bellow:

Procedure for granting patents or PoA

1. Filing the application together with all necessary particulars to render it 'regular filing' (in other words for a filing date to be accorded).

[36] http://www.obi.gr/obi/

2. A 4-month term for any corrections to be made or omissions to be supplemented to render it ‘regular filing’.
3. An examination of whether the invention is ‘new’ and ‘involves an inventive step’– preparation of the search report.
4. A 3-month term for comments by the applicant on the search report.
5. Preparation of the final search report.
6. Grant of the patent or PoA.

Procedure for granting UMC’s

1. Filing of the application (or request to convert patent application before patent grant into a UMC application or automatic conversion by OBI due to late payment of search report preparation fees).
2. A 4-month term for any corrections to be made or omissions to be supplemented to render it ‘regular filing’.
3. Granting of the UMC (without prior examination of whether new or industrially applicable – this is the applicant’s responsibility).

Preparing a Patent, PoA or UMC application

Once an interested party has decided which protection title (patent, PoA, UMC) he wishes to register his invention under in Greece he should prepare his application in such a way that full protection of his rights is afforded.

To this end, he should pay particular attention to preparing the description and any drawings, claims and the abstract. The description and any drawings are used in the disclosure of the invention.

The claims determine the extent and content of the protection requested based on the invention’s technical features only. The invention abstract does not affect the extent and content of the protection requested because it is used solely to provide technical information.

Thus interested parties should bear the following points in mind:

1. The invention must be disclosed:

The patent, PoA or UMC application should disclose the invention in a clear, complete manner so that its practical application by an expert is possible. The protection afforded upon grant of patent, PoA or UMC relates solely to what has been disclosed. Note that if the invention disclosure is inadequate to permit its application by an expert there are grounds for invalidating the patent, PoA or UMC following a court ruling. Such as ruling may be sought by a competitor.

Care should taken so that the abstract and any drawings include all necessary information relating to the invention because following filing of the application no addition to the scope of invention is possible.

2. There must be unity of invention:

The patent, PoA or UMC application should refer to one invention or more than one which are connected to each other so as to constitute a unity of invention. Examples of inventions constituting a unity of invention are:

(i) A product, the manufacturing method for that product and uses for it,

(ii) A method and apparatus or means for implementing that method,

(iii) A product, method for producing it and apparatus or means specifically for implementing that method.

If the patent, PoA or UMC application relates to more than one unconnected invention (composite application) the applicant may divide the application into several discrete applications while retaining the initial application date as the filing date for each section of the application. Such severance may be done up until the grant of patent, PoA or UMC.

3.2.6 Spain

In Spain there are Software Certifications for almost anything. Each brand and/or manufacturer of certain importance issues their own certification schemes (Redhat, Sybase, HP, Adobe, Verisign, Microsoft, Salesforce…

While big companies (CapGemini, Accenture, Indras, Atos, are usually proficient in one of the most renowned methodologies around as CMMI (Capability Maturity Model Integration)[37] or the PMBOK (Project Management Body of Knowledge of the Project Management Institute) or PRINCE2, a de facto standard used extensively by the UK Government and widely recognised and used in the private sector, both in the UK and internationally.

These same big companies offer and act themselves also as Certification Centers. Spain acts as a gateway both to Europe and Latin America and this is one of the reasons why big companies establish Delivery Centers here, to offer clients competitive, high-quality technology services that enhance their business performance.

On the other hand, the Ministry of Public Administrations of Spain, in order to promote eGovernment and encourage the use of the new citizen´s Electronic Identity Card, has set up a MultiPKI Validation Platform (MPVP) that provides free Electronic Identity and Signature Services (eID Services) to eGovernment Applications. These eID services are applicable to all the qualified electronic certificates issued by all the Certification Service Providers accredited in Spain, included the two qualified certificates of the citizen´s eID card. The service is available to all eGovernment applications of the country that can benefit of incorporating eIDs and eSignature functions in their administrative procedures.

The FLOSS initiative in Spain

In Spain, free software and open source solutions have been consolidated as a viable alternative to commercial software. The technological independence and the advantages related to the access to the source code have meant a revolution. The use of Free/Libre and Open Source Software (FLOSS) has been welcomed in Public Administrations and some Regional Governments have launched significant initiatives (Extremadura 2003, the LinEx project)) serving as a best practice case for the rest of Europe)

[37] CMMi is a process improvement approach that provides organizations with the essential elements of effective processes that ultimately improve their performance. The CMMi appraisal is a certification granted by the Software Engineering Institute (SEI), a U.S. Department of Defense federally funded research and development center operated by Carnegie Mellon University. The certification is based on two main criteria: product or system quality and the maturity of the organizations in software development .the creation of specialized employment to deliver high quality services to clients

In March 2010, LPI-Spain (Linux Professional Institute) the world's premier Linux certification organization, announced its partnership with “Proyecto Universidad Empresa” (PUE) to promote LPI certification and training within Spain's public schools. PUE is Spain's leading agency in the development of IT training and certification and provides academic programs for such major IT organizations as Microsoft, Cisco and Sun.

LPI endeavors to work with academic organizations and government agencies around the world to promote the adoption of Linux and Open Source. The Linux Professional Institute is globally supported by the IT industry, enterprise customers, community professionals, government entities and the educational community. LPI's certification program is supported by an affiliate network spanning five continents and is distributed worldwide in multiple languages in more than 7,000 testing locations. Since 1999, LPI has delivered over 230,000 exams and 75,000 LPIC certifications around the world.

Under this initiative with PUE, LPI-Spain will promote the LPI Approved Academic Partnership (LPI-AAP) program with public sector education programs in Spain to ensure high quality Linux training and certification.

On 8 January 2010, Spain has adopted the Royal Decree 4/2010 which implements the National Interoperability Framework planned in the eGovernment Law 11/2007. The framework has been developed with the participation of all Public Administrations (General State, Regional and Local governments - represented by one hundred experts) and of the ICT Industry professional associations. The Decree includes important provisions, especially Articles 16 and 17 related to the reuse of Public Sector software, the applicable licensing condition and the use of software repositories or forges.

According to Article 16.1, the licensing conditions of applications owned by Public Administrations and that can be made available for other Public Administrations or for the citizens, must allow the free use/reuse of these applications. Licensing conditions must also exclude the software appropriation by a third party and protect the administration from liability, support and warranty obligations.

However, there is no general obligation to distribute all Public Sector software: this is left to the appreciation of the administration (depending on the interest and potential reusability of the solution by other public sector agencies and by the civil society). However, if the distribution is decided, it must be under open source conditions (combined with strong copyright conditions for avoiding the exclusive appropriation that would happen if the software could become proprietary).

STANDARDS IN SPAIN

Spain has established specific certification for certain products. This "homologation" involves cumbersome product testing by approved laboratories. However, a product that meets the standards and certification requirements of any other EU country can be imported and sold in Spain without further testing. Spanish homologation requirements remain in force for computer keyboards and screens, dot matrix printers, teleprinters, medical equipment, electric typewriters, telecommunications equipment, motor vehicles, bicycles, pleasure boats, gas connectors, etc.

The Spanish Standards Certification Association (AENOR = Asociacion Española de Normalizacion y Certificacion) is responsible for developing voluntary standards and certification programs. It represents Spain in international standards institutions. The Spanish government publishes a list of approved laboratories for testing and certification each year.

Established in 1986 as a non-profit private association, the Asociación Española de Normalización y Certificación (AENOR) undertook the responsibility formerly held by official authorities for the development, publication and promotion of Spanish standards (UNE standards), for which it has been granted recognition by law as the only body responsible. Being an active member of the main European and international standardization, AENOR's mission is to contribute, through the development of Standardization and Certification, to the improvement of quality within companies and also of their products and services, as well as to protect the environment and, therefore, the well-being of society.

Concerning certification activities, AENOR has been accredited as a certification entity by the Spanish National Accreditation Body (ENAC) as far as the certification of both quality and environmental management systems are concerned and certification of products and services according to national standards.

Spain now allows the entry of used equipment, material and goods. However, they are subject to the same standards concerning safety as apply to any new import. Additionally, there may exist regulations specific to the particular type of equipment, such as computers and peripherals that is being imported.

Labeling, Marking Requirements

Country of Origin Marking

Every article entering Spain must be marked with the name of the country of origin in any official language, preferably in Spanish, unless an exception of marking is provided for in the law. The country of origin is the country of manufacture, production, or growth of the article. The requirement applies to each unit unless exempted. The phrase "made in" is required only in the case where the name of any locality other than the country or locality in which the article was manufactured appears on the article or its container. The marking "made in (country), "product of (country)", or other words of similar meaning must appear in close proximity to and in comparable size letters of the other locality to avoid possible confusion. When marking is not feasible, such as when the article is too small or marking would in some way damage the merchandise, then the packaging or container that will reach the final consumer must be marked.

Besides this generalization, there are specific categories of goods, for which marking, labeling, and/or testing requirements are applicable in Spain, although we will mention only here the CE Marking because it is the one that could be more affected by devices used in LLM.

CE Marking

The CE (Conformité Européenne) Marking is required to be displayed on regulated products offered for commercial sale on the European market. It indicates that a product complies with applicable European Directives related to health, safety, environment and consumer protection. Because the CE Marking identifies products that meet a common set of criteria established and adopted by the 15 CE members, the CE Marking on your products will permit them to move freely in commerce throughout the European market. The manufacturer, or authorized representative, is responsible for placing the CE Marking on compliant products. The common CE Marking logo is placed on the product, product literature or packaging as described in each Directive. Articles regulated under the European Directives that are not properly marked when imported are subject to delay in customs and may not be cleared for consumption.

In addition, the Certification Body is accredited by ENAC (Entidad Nacional de Acreditación), in accordance with the requirements laid out in the standard UNE-EN 45011:1998 for product certification.

ENAC (Entidad Nacional de Acreditación) is the body designated by the Government to assess technical competence in accordance with international standards.

The purpose of ENAC is to build trust in the market and in the wider community in relation to the technical competence of accredited conformity assessors, thus contributing to people's safety and welfare, the quality of products and services, and environmental protection, and thereby to the increased competitiveness of Spanish products and services and to a reduction in the costs for society due to these activities.

To perform its function, **ENAC** carries out the following activities:

- Declaring technical competence of conformity assessors through an independent, impartial and transparent assessment system based on international criteria.
- Promoting international acceptance of activities of accredited conformity assessors by arranging recognition agreements, thus facilitating business exchanges in a global marketplace.
- Cooperating with government and other accreditation user organizations, assuring that the accreditation service that they are going to make use of meets their needs.
- Offering conformity assessors a high value-added service that represents a differential feature in the market by being a guarantee of integrity and competence and thus increasing business opportunities and inspiring public confidence in their activities.
- Managing the accreditation system with efficacy criteria and in keeping with client needs.
- Furthering and disseminating accreditation criteria and procedures to assist conformity assessors in their access to accreditation and publicize the concept of accreditation and ENAC activities and its accredited bodies to all stakeholders.
- Cooperating with national and international institutions and organisations on aspects relating to its aims and objectives.

eIdentification/eAuthentication:

Public Certification Authority

The Spanish Government has set up a Public Certification Authority (CERtificación ESpañola – CERES) operated by the National Mint (Fábrica Nacional de Moneda y Timbre). CERES issues digital certificates to be used in electronic administrative transactions.

National eID card - DNIe

The Government introduced electronic cards containing biometric identifiers and electronic signatures in 2006.

The national eID card makes it possible to digitally sign electronic documents and contracts, identify and authenticate citizens in a secure digital environment and provide them with easy, straightforward, fast and convenient access to eServices. The card's validity period is of 10 years.

Today most of the Public Administrations (Central Government, Regions and Municipalities) and businesses provide eServices enabling the use of the DNIe. Among the most popular of these services are: tax filing, application for employment benefits, accessing personal data in public registers, request for and reception of a form, tax payment, online banking, and many more.

On 13 March 2009, the Council of Ministers gave the green light to a €14 million investment in a series of actions set to generalise the use of the national eID card and to stimulate the spread of reliable digital services and applications. The related “agreement for the promotion of the DNIe” signed, in June 2007, between the State-owned company 'Red.es' and the State Secretariat for Telecommunications and the Information Society, has furthermore been extended up to 31 December 2010. The new investment comes in addition to approximately €43 million spent under this agreement.

On 30 July 2009, the Ministry of Industry, Tourism and Trade along with the Ministry of Interior and the Ministry of the Presidency signed with companies of the IT sector a collaboration agreement aimed at enhancing the use of the DNIe. Among other actions, this agreement provides for the promotion among the manufacturing and selling companies of the incorporation of DNIe card readers in the new models of computers, mobiles devices and other electronic tools that will be commercialised.

The State Secretariat of Telecommunications and the Information Society (SETSI) announced on 26 October 2009 the launch of an action plan aimed at promoting the use of the national eID card (DNIe) among citizens and businesses while enhancing the offer of reliable services and applications requiring the use of the card.

The implementation of the DNIe is part of the 'Avanza2' Plan.

@firma - MultiPKI Validation Platform for eID and eSignature Services

The former Ministry of Public Administrations (replaced by the Ministry of the Presidency), in order to promote eGovernment and encourage the use of the eID card, set up this multiPKI validation platform (MPVP - @firma) that provides free eID services to eGovernment applications.

Since 2006, the platform has been providing a secure service to verify the state and validity of the qualified certificates used by citizens and companies in any eGovernment service.

These eID services are applicable to all the qualified electronic certificates issued by all the Certification Service Providers accredited in Spain, including the two qualified certificates of the citizen´s eID card. The service is available to all eGovernment applications of the country that can benefit from incorporating eIDs and eSignature functions in their administrative procedures.

4 Interoperability

The aim of this paragraph is to describe the integration schema introduced by the LLM system and the requirements that third-party applications have to satisfy in order to allow for their consistent cooperation with the LLM system. Furthermore, conformance metrics and guidelines will be defined in order to let interest parties identify and test whether their application could be a candidate component to be integrated into the LLM platform. Conforming to most of the below mentioned requirements, will automatically provide stand-alone applications to be integrated to our system.

As already mentioned in Deliverables 3.1 and 3.2, LLM system is comprised of three independent components: the CTC, Cognitive Training Component, the PTC, Physical Training Component and the ILC, Independent Living Component. These three independent components will meet the proposed service by means of a server side system, which is comprised of a database and a web service and a set of PC-based applications which is the core element of the LLM service, the Central Management System (CMS).

Therefore in order for an application to be compatible with the LLM system we should examine what is needed for its successful interoperability with both the LLMWS/LLMDB and the LLM CMS, which constitute the core of the LLM system.

4.1 LLMWS - LLMDB integration guidelines and conformance metrics

The integration aspects of the system and especially the data information exchange are tackled on the basis of a web service and a database. The LLMWS is responsible for providing all methods and functions in order to support the three independent components' and CMS's functions, (see Figure 2).

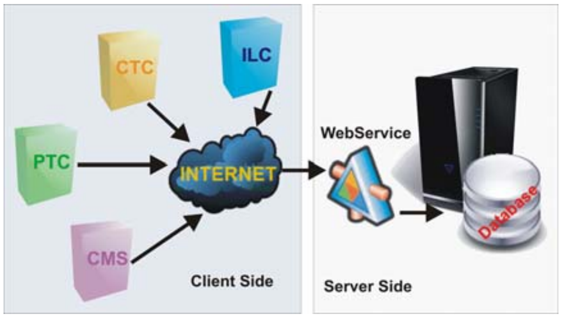

Figure 2 The web service supports the three independent components

A database accompanies and supports the web service's procedures. Each of the three components accomplishes a different scope of application and provides heterogeneous data and semantic sources. According to these requirements the proposed architecture must support the integration of the data and the co-ordination of the components' functionalities.

One of the major features that the proposed architecture should accomplish is flexibility and loose-coupling. The web service's architecture and functionality is open in order to allow new developments to be integrated and supported by the proposed service in the future developed components (CTC, PTC, ILC). The prerequisite for the candidate applications to be integrated into the proposed service is to be compatible with the general framework of the service and be able to store their data to the LLMDB via LLMWS Soap API.

Web service interoperability goals are to provide seamless and automatic connections from one software application to another. SOAP, WSDL, and UDDI protocols define a self-describing way to discover and call a method in a software application -- regardless of location or platform. Data is organized into XML request and response documents and moved between software packages using HTTP or message-based protocols. The HTTP protocol that plays the role of the communication layer in conjunction with XML messages using this layer the web services are platform and firewall independent.

Web Services use Extensible Markup Language (XML) messages that follow the SOAP standard and have been popular with traditional enterprise. In such systems, there is often a machine-readable description of the operations offered by the service written in the Web Services Description Language (WSDL).

The web service provides structures (an example is given in Table 1) as inputs and outputs to all supported methods. All structures and methods are well described by a human readable document already publicly available, the LLM Developer Reference. An example of a data structure that describes a senior entity is given below as an example.

```
<s:complexType name="senior">
   <s:sequence>
      <s:element minOccurs="1" maxOccurs="1" name="senior_id" type="s:int"/>
      <s:element minOccurs="0" maxOc-curs="1" name="lname" type="s:string"/>
      <s:element minOccurs="1" maxOccurs="1" name="birthdate"
type="s:dateTime"/>
……………………………………………...
   </s:sequence>
</s:complexType>
```

Following, a list with all conformance metrics is addressed, explaining through examples the way a candidate component should test if they are applicable to its case:

- Component developers **must** satisfy the SOAP exchanging messages prerequisites for interacting and exchanging information with the LLM system, as LLMWS is designed according to the SOAP envelope architecture. *(obligatory)* A typical format of a SOAP envelope is listed below:

```
<?xml version="1.0"?>
<soap:Envelope
         xmlns:soap="http://www.w3.org/2001/12/soap-envelope"
         soap:encodingStyle="http://www.w3.org/2001/12/soap-encoding">
         Message information goes here
</soap:Envelope>
```

- Each one of the three independent components **must** be able to store their data in the LLMDB (training performance results for the case of PTC and/or CTC and any alarms detected regarding the ILC) according to LLMWS certain data structures. Three different data structures have been introduced by the LLMWS to deal with the rationale and data semantics each component has to offer.

ILCSeniorActivity Data Structure

```
<s:complexType name="ILCSeniorActivity">
<s:sequence>
<s:element minOccurs="1" maxOccurs="1" name="ID" type="s:int"/>
<s:element minOccurs="1" maxOccurs="1" name="senior_id" type="s:int"/>
<s:element minOccurs="0" maxOccurs="1" name="seniorslname" type="s:string"/>
<s:element minOccurs="0" maxOccurs="1" name="seniorsfname" type="s:string"/>
<s:element minOccurs="1" maxOccurs="1" name="ilcactivityid" type="s:int"/>
<s:element minOccurs="0" maxOccurs="1" name="ilcactivityname" type="s:string"/>
<s:element minOccurs="1" maxOccurs="1" name="ilcid" type="s:int"/>
<s:element minOccurs="0" maxOccurs="1" name="ilcname" type="s:string"/>
<s:element minOccurs="1" maxOccurs="1" name="datetimestart"
type="s:dateTime"/>
<s:element minOccurs="1" maxOccurs="1" name="datetimeend"
type="s:dateTime"/>
<s:element minOccurs="0" maxOccurs="1" name="score" type="s:string"/>
<s:element minOccurs="1" maxOccurs="1" name="level" type="s:int"/>
</s:sequence>
</s:complexType>
```

CTCSeniorActivity Data Structure

```
<s:complexType name="CTCSeniorActivity">
<s:sequence>
<s:element minOccurs="1" maxOccurs="1" name="ID" type="s:int"/>
<s:element minOccurs="1" maxOccurs="1" name="senior_id" type="s:int"/>
<s:element minOccurs="0" maxOccurs="1" name="seniorslname" type="s:string"/>
<s:element minOccurs="0" maxOccurs="1" name="seniorsfname" type="s:string"/>
<s:element minOccurs="1" maxOccurs="1" name="ctcactivityid" type="s:int"/>
<s:element minOccurs="0" maxOccurs="1" name="ctcactivityname"
type="s:string"/>
<s:element minOccurs="1" maxOccurs="1" name="ctcid" type="s:int"/>
<s:element minOccurs="0" maxOccurs="1" name="ctcname" type="s:string"/>
<s:element minOccurs="1" maxOccurs="1" name="datetimestart"
type="s:dateTime"/>
<s:element minOccurs="1" maxOccurs="1" name="datetimeend"
type="s:dateTime"/>
<s:element minOccurs="0" maxOccurs="1" name="score" type="s:string"/>
<s:element minOccurs="1" maxOccurs="1" name="level" type="s:int"/>
```

```
</s:sequence>
</s:complexType>
```

PTCSeniorActivity Data Structure

```
<s:complexType name="PTCSeniorActivity">
<s:sequence>
<s:element minOccurs="1" maxOccurs="1" name="ID" type="s:int"/>
<s:element minOccurs="1" maxOccurs="1" name="senior_id" type="s:int"/>
<s:element minOccurs="0" maxOccurs="1" name="seniorslname" type="s:string"/>
<s:element minOccurs="0" maxOccurs="1" name="seniorsfname" type="s:string"/>
<s:element minOccurs="1" maxOccurs="1" name="ptcactivityid" type="s:int"/>
<s:element minOccurs="0" maxOccurs="1" name="ptcactivityname"
type="s:string"/>
<s:element minOccurs="1" maxOccurs="1" name="ptcid" type="s:int"/>
<s:element minOccurs="0" maxOccurs="1" name="ptcname" type="s:string"/>
<s:element minOccurs="1" maxOccurs="1" name="datetimestart"
type="s:dateTime"/>
<s:element minOccurs="1" maxOccurs="1" name="datetimeend"
type="s:dateTime"/>
<s:element minOccurs="0" maxOccurs="1" name="score" type="s:string"/>
<s:element minOccurs="1" maxOccurs="1" name="level" type="s:int"/>
</s:sequence>
</s:complexType>
```

As it can be easily derived from above, there are certain attributes that are essential to be provided by the components and stored to the LLMDB. These are the following:

- **Senior_id**, the identification code of the senior performing the training or producing an alarm.
- **Xxcactivityid**, the identification code of the physical/cognitive activity performed by the senior or the type of alarm that he produced.
- **XXCid**, the identification code of the xxc component that is used for performing the specific activity (e.g. BrainFitness or Gradior)
- **Datetimestart**, the date and time the activity started
- **Datetimeend**, the date and time the activity ended
- **Level**, difficulty level of the activity

These data are needed in order to provide LLM system with the performance progress of the senior and their presence is considered of **utmost importance** to the successful integration of the components into the overall LLM service. *(obligatory)*

- SSL encryption **must** be accepted by a client in order to gain access to the LLM data. Moreover, the client must accept the LLM System's certificate for a successful encrypted connection. Although LLM System doesn't manage personal information, the data transferring is encrypted with SSL. *(obligatory)*

- Support of already existing activities or introduction of new ones in the LLMDB. The components' providers **must** be able to identify which activities of the already existing, they support, and in case there are additional activities recorded by their software or hardware, then these need to be forwarded to the LLM administrators (including all the appropriate information such as **activity name** and **units of measurement**) in order to be placed into the LLMDB. This kind of information needs to be stored by the administrator just once and this will be part of the preliminary stage of integration process of a third-party application to the LLM system. The new activities introduced by a new component provider should also be checked by the LLM scientific stuff, so to ensure that there is no overlapping or conflict between the newly introduced activities and the already existing ones. *(obligatory)*

- Each activity **must** be meaningful, by means of targeting to a specific function (either cognitive or physical fitness function). An activity stored in LLMDB might comprise of just a single or multiple tasks. For example a running task and a cycling task both focus on training a participant's aerobic endurance, therefore their combination could be considered as single activity called "Aerobic endurance". Each component's provider should be able to discriminate whether a single task (exercise) or a combination of more than one tasks (exercises) target to the training of a specific function (cognitive or physical) and take into account possible recommendations of the LLM scientific board regarding the correct incorporation of each activity. *(obligatory)*

- Result data that will be stored into the LLMDB, **must** be as generic as possible. This means that, each component that records performance results using its internal logic of assessment, needs to redefine the score to be stored in LLMDB (calculate an overall/average score), as it might be derived from a group of single tasks already described above. *(obligatory)*

- According to the LLM design strategy, components shall store to the LLM Database (through the LLMWS) meaningful data of activities (set of tasks). These activities shall provide a meaningful result for a cognitive or physical task of a person. Taking into consideration that a test (testing set of tasks) providing such results cannot be achieved in less than 10 seconds, a component (having a specific senior logged in) **must not** do calls to the web service more frequent than 10 seconds. *(obligatory)*

- Credentials (username and password) are **obligated** for each data access. This ensures that a user will act only with the role he is assigned to. This ensures that only authorized people can access (read/write/delete) any kind of information. *(obligatory)*

- Each component's available activities **might** cover as most cognitive or physical functions as possible. By this way, the component will be able to provide better understanding on the overall health status of a senior participant. *(optional)*

4.2 LLMCMS integration guidelines and conformance metrics

Applications to be integrated into the LLM system should also fulfill a number of requirements posed by the LLMCMS component, the LLF - LLM system local user interface framework. These are the following:

- The Windows message-queue must be processed properly by every window of the application (e.g. no modal dialogues). *(obligatory)*
- The Application shall not have problems when it's forced to change window-format or switch to fore-/background. *(obligatory)*
- The bottom left and right corners of the screen are reserved for LLF-Buttons (Back and Alarm) and should not intersect with Application Buttons / areas of interest. *(obligatory)*
- Applications can’t use any of the following ports: 8003, 5800, 5900, as they are reserved by the LLF application. *(obligatory)*
- An Application can be "killed" by the LLF (e.g. when pressing the "back" button) and therefore it shall store its training results as often as reasonable. *(optional)*
- If an application passes senior-related data about the senior who is logged into the CMS to the LLMWS, the appropriate senior-id will be provided by the LLF through command line arguments during startup call. The application must be able to accept this id. *(optional)*

5 ISSUES OF LIABILITY

There are various issues to be addressed when developing software in general, as well as when this software is addressed to elderly people.

Concerning security issues, it seems easier to secure the infrastructure, communication and physical layers and much more difficult to do the same for the application level, since this requires much more expertise on the part of the application designers and programmers. It is nearly impossible to deliver a bug-free application if a proper and organized process is not implemented. What's more, implementing security without a clear process can be based on inefficient processes, and insufficient internal communication between teams regarding relevant security issues.

As a result, normal day-to-day insecure products have many implementations and designs that may, if they are not implemented correctly, introduce security flaws and open the door for system users, legitimate or malicious hackers, to perform unauthorized operations. Exploiting these security breaches, intentionally or unintentionally, may harm the three crucial information security missions of every organization – preserving the availability, integrity, and confidentiality of the organization's sensitive data.

ISO 27001 - "Information Security Management - Specification With Guidance for Use" has as a basic objective to help establish and maintain an effective information management system, using a continual improvement approach. It implements OECD (Organization for Economic Cooperation and Development) principles, governing security of information and network systems.

The following are some of the most important security policies aligned with the standard (http://www.27001-online.com/secpols.htm):

Chapter ONE - INFORMATION SECURITY ORGANIZATION
Chapter TWO - CLASSIFYING INFORMATION AND DATA
Setting Classification Standards
Defining Information
Classifying Information
Accepting Ownership for Classified Information
Labelling Classified Information
Storing and Handling Classified Information
Isolating Top Secret Information
Managing Network Security
Chapter THREE - CONTROLLING ACCESS TO INFORMATION AND SYSTEMS
Controlling Access to Information and Systems
Chapter FOUR - PROCESSING INFORMATION AND DOCUMENTS
Networks
System Operations and Administration
Data Management
Transferring and Exchanging Data
Permitting Emergency Data Amendment
Receiving Information on Disks
Setting up a New Folder / Directory
Amending Directory Structures

Sharing Data on Project Management Systems
Archiving Documents
Information Retention Policy
Setting up New Spreadsheets
Setting up New Databases
Linking Information between Documents and Files
Updating Draft Reports
Deleting Draft Reports
Using Version Control Systems
Updating Customer Information
Using Meaningful File Names
Managing Data Storage
Managing Databases
Using Headers and Footers
Using and Deleting ‘Temp’ Files
Using Customer and Other Third Party Data Files
Saving Data / Information by Individual Users
Backup, Recovery and Archiving
Document Handling
Securing Data
Chapter FIVE - PURCHASING AND MAINTAINING COMMERCIAL SOFTWARE
Chapter SIX - SECURING HARDWARE, PERIPHERALS AND OTHER EQUIPMENT
Chapter SEVEN - COMBATING CYBER CRIME
Chapter EIGHT - CONTROLLING E-COMMERCE INFORMATION SECURITY
Chapter NINE - DEVELOPING AND MAINTAINING IN-HOUSE SOFTWARE
Controlling Software Code
Software Development
Testing & Training
Documentation
Chapter TEN - DEALING WITH PREMISES RELATED CONSIDERATIONS
Chapter ELEVEN - ADDRESSING PERSONNEL ISSUES RELATING TO SECURITY
Chapter TWELVE - DELIVERING TRAINING AND STAFF AWARENESS
Chapter THIRTEEN - COMPLYING WITH LEGAL AND POLICY REQUIREMENTS
Complying with Legal Obligations
Complying with Policies
Avoiding Litigation
Chapter FOURTEEN - DETECTING AND RESPONDING TO IS INCIDENTS
Chapter FIFTEEN - PLANNING FOR BUSINESS CONTINUITY
Business Continuity Management
Initiating the Business Continuity Project
Assessing the Business Continuity Security Risk
Developing the Business Continuity Plan
Testing the Business Continuity Plan
Training and Staff Awareness on Business Continuity

Maintaining and Updating the Business Continuity Plan
Realistic Testing Environment for Business Continuity Plans
Impact of the Pace of change on the Business Continuity Plan

From all the above policies concerning liability, special care has been taken to address issues emerging during the execution of the trials, as well as the preparation and launching of the end-product for market exploitation at the end. More particularly, during the execution of the trials, special care has been taken so as to ensure:

- the participating partners insurance coverage.
- the national sanitary agencies' demands as regards the protection of participants in trials, including specific insurance policies in some cases.
- respect of local rules concerning trials.
- having health professionals supervising the trials locally, which will lower risks, and reinforce liability.

During the development of the LLM services and the trial period, special care has been taken to ensure:

- accurate and strictly factual project dissemination information
- careful interpretation of the data emerging from the trials
  Finally, before proceeding with market exploitation, the following issues would be addressed to ensure liability:
- The "reality" behind LLM's offer (facts, wording, commercial promise, etc.)
- The position of the final service/system offered to the market vis à vis potential prescribers, users, or customers, etc.
- The final service offered for selling will have to conform to local laws, rules and regulations of all the markets involved.

Specific organisations in each country (e.g. the Laboratoire National d'Essais (LNE) in France, and probably KemaKeur in the Netherlands, TÜV in Germany, etc) be consulted on both technical and legal of the technical and legal -legal aspects regarding the liability of the end product.