FUTURE INTERNET PPP

fi star

THE FUTURE. NOW.

Deliverable D2.1

Standardisation and Certification requirements

Editor:	Franck Le Gall, easy global markets
Deliverable nature:	Report (R)
Dissemination level: (Confidentiality)	Public (PU)
Contractual delivery date:	Dec. 2013
Actual delivery date:	Jan. 2014
Suggested readers:	
Version:	1.1
Total number of pages:	74
Keywords:	Standardisation, certification

Abstract

This document details the technical requirements resulting from existing standards and prepares future certification process.

Disclaimer

This document contains material, which is the copyright of certain FI-STAR consortium parties, and may not be reproduced or copied without permission.

All FI-STAR consortium parties have agreed to full publication of this document.

The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the FI-STAR consortium as a whole, nor a certain part of the FI-STAR consortium, warrant that the information contained in this document is capable of use, nor that use of the information is free from risk, accepting no liability for loss or damage suffered by any person using this information.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 604691.

Impressum

[Full project title] Future Internet Social and Technological Alignment Research

[Short project title] FI-STAR

[Number and title of work-package] WP1 Requirements Specification

[Number and title of task] T1.2 Standardization and certification requirements analysis

[Document title] Standardisation and Certification requirements

[Editor: Name, company] Franck Le Gall, easy global markets

[Work-package leader: Name, company] Christoph Thuemmler, Edinburgh Napier University

[Estimation of PM spent on the Deliverable] 40 PM

Copyright notice

Executive summary

The “Standardization and Certification Requirements Report” is the deliverable D1.2 of project FI-STAR. The report defines the requirements related to standardisation and certification the project would have to comply with. In the contexts of eHealth and FI-PPP, it provides an analysis of the standardisation landscape in five areas being:

1. Development of a software product,
2. Interoperability of the product with other products,
3. Usage of the product by a human user,
4. Resilience to protect from harm, and
5. Data security

As far are standardisation requirements concerned, FI-STAR has to pay more attention to the eHealth domain as general standardisation is treated at the FI-PPP level. On the contrary, as far certification requirements are concerned, FI-STAR has to pay more attention to the FI-PPP domain. Nothing is really implemented within the programme whereas many activities in certification and interoperability validation exist in the eHealth.

Regarding standardisation, a large part of the work presented is thus the identification of the health standards relevant for the project as well as to identify the areas where FI-STAR contribution would make sense. These include:

1. Overall interoperability issues in particular at the semantic (data and content/meaning) level
2. Support validation and certification with implementation done in WP6
3. Work smoothly with the technical platforms, with WP6 support and FI-WG on standardisation

In order to reuse very important work from previous and current projects, a profile based approach is proposed. Profiles reduce the complexity of the implementation of the communication functions or use cases by specifying a subset of standards that limit and precise their usage for the specific needs. Profiles are thus standards-based choices in different levels such as application interfaces, protocols for communication, security level, file format, and semantic. They are generally defined for the integration purpose and provide developers with a clear implementation path for communication standards. Profiles

Reference profiles for the PAN, LAN, WAN and HRN interfaces, applicable to use cases that the objectives are the monitoring of patient information using devices and mobile applications (BPTM, CR, CDTA, DSS, TS) have been identified. They are detailed for data/messages, semantic, transport and communication protocol and security parts.

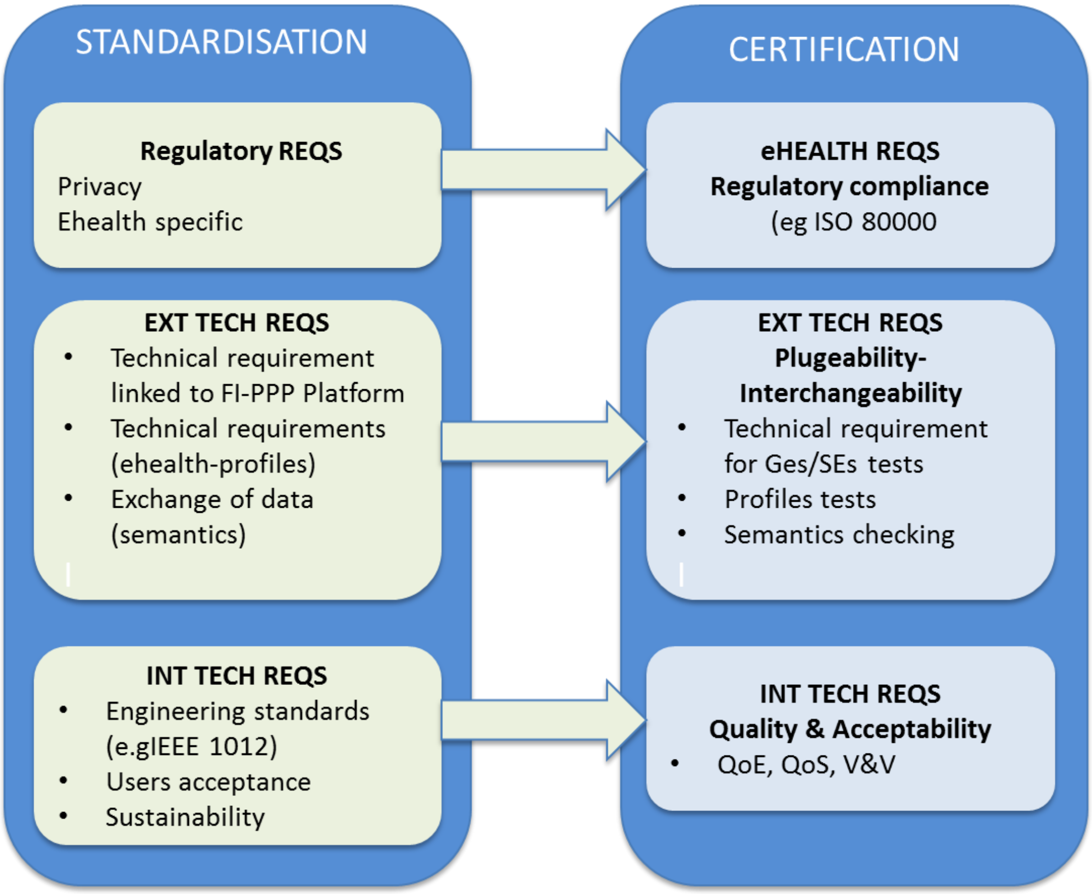
On the certification and validation aspects, a strategy for FI-STAR which provides easy and simple proof of compliance to requirements to the market is proposed. This strategy is pragmatic while complying with the existing regulatory framework, helping the issuing of high quality and sustainable outcomes by the project FI-STAR and the FI-PPP programme. Three different approaches are proposed depending on the level of the considered requirements:

- **Regulatory requirements**: there is no other choice than ensuring the regulatory compliance of systems, devices and applications put on the market by the project FI-STAR. Nevertheless, this is usual business of the health IT providers being present in the project and thus does not require project specific attention.
- **External requirements**: these requirements comes from third parties, external to the project and does not contain mandatory requirements of standardization or certification of IT products or IT-based services. Motivation for certification is thus mostly guided by interoperability interests (also here as also promoted as interchangeability and plugability) : FI-STAR developers want to benefit from components (GEs) from the FI-PPP that are in-line with their specification while FI-STAR wishes to develop platforms that are re-useable by

third parties (SEs) and which can connect and exchange data with medical systems. In that case, 2 options exist

- **Validation of GEs/SEs**: this is not provided by any third party today and thus has to be conducted at the FI-STAR level and promoted at the FI-PPP level. This activity is being driven with WP6.
- **Interoperability with health systems**: many profiles based interoperability schemes and tools are already promoted by many EU projects and Fi-STAR has to capitalize on this important existing offers. It should be conducted on a voluntary basis. For instance Projectathon organised in the framework of connectathon is one of the most efficient way to expose FI-STAR outcome to the health market reality. Such activity has to be done by development teams within FI-STAR with the support of dissemination and exploitation teams. Other offers are developed within the eHealth thematic network Antilope

- **Internal requirements**: while we need to communicate with the external world, we need to be sure what we deliver has high quality and is conform to the expectation (also from users' side). Quality improvement has to be sought to increase the acceptability of FI-STAR outcomes. The project thus has to set its own quality requirements and deploy its internal processes to monitor them. These requirements are described within the quality assessment framework given in D6.1.



Simplified overview of Standardisation and Certification requirements in FI-STAR

List of authors

Company	**Author**
EGM	Philippe Cousin
EGM	Karima Bourquard
BTH	Samuel Fricker
EGM	Franck Le Gall
TiU	Nadezhda Purtova
TiU	Eleni Kosta
ALL	Contribution to Healthcom 2013

Table of Contents

List of figures

List of tables

Abbreviations

BPTM	Bipolar Patient Treatment Management Solution
CDTA	Chronic disease Treatment Assistance
CEN	European Committee for standardization
CENELEC	European Committee for electrotechnical standardization
CR	Cardiac Rehabilitation
DSMS	Drug Supply Manager Solution
DSS	Diabetes Share System
ETSI	European Telecommunications Standards Institute
GE	Generic Enabler
GITB	Global eBusiness Interoperability Test Bed
HRN	Health Reporting Network
IHE	Integrating the Health enterprise
IHE ATNA	IHE Audit trace and Node Authentication
IHE CT	IHE Consistent Time Integration
IHE IUA	IHE Internet User Authorization
IHE RTM	IHE Rosetta Terminology Mapping
IHE XCA	IHE Cross Community Access
IHE XCF	IHE Cross Community Fetch
IHE XCPD	IHE Cross Community Patient Discovery
IHE XDR	IHE Cross Enterprise Reliable Interchange
ISO	International Organization for Standardization
LAN	Local Area Network
MDD	(European) Medical Device Directive
MDF	(European) Medical Device Framework
PAN	Personal Area Network
SAML	Security assertion markup language
SE	Specific Enabler

TMS	Operating Theatre monitor Solution
TS	Telecare Solution
USDL	Unified Service Description Language
WAN	Wide Area Network

Definitions

Term	Definition	Reference document
Conformity assessment	Any activity concerned with determining directly or indirectly that relevant requirements are fulfilled. NOTE: Typical examples of conformity assessment activities are sampling, testing and inspection; evaluation, verification and assurance of conformity (supplier's declaration, certification); registration and approval as well as their combinations.	ISO/IEC 17000:2004
Conformity assessment scheme	Conformity assessment system as related to specified products, processes or services to which the same particular standards and rules, and the same procedure, apply.	ISO/IEC 17000:2004
Conformity evaluation	Systematic examination of the extent to which a product, process or services fulfils specified requirements.	ISO/IEC 17000:2004
Conformity testing	Conformity evaluation by means of testing	ISO/IEC 17000:2004
Harmonised standard	Technical specification adopted by European Standards Organisations, developed under a mandate given by the European Commission and/or European Free Trade Association, in support of essential requirements of a New Approach Directives	
Interoperability	The ability of two or more systems or components to exchange data and use information.	ETSI White Paper No. 3
Interoperability (Technical)	Usually associated with hardware/software components, systems and platforms that enable machine-to-machine communication to take place. This kind of interoperability is often centred on (communication) protocols and the infrastructure needed for those protocols to operate.	ETSI White Paper No. 3
Interoperability (Syntactical)	Usually associated with data formats. Certainly, the messages transferred by communication protocols need to have a well-defined syntax and encoding, even if it is only in the form of bit-tables. However, many protocols carry data or content, and this can be represented using high-level transfer syntaxes such as HTML, XML or ASN.	ETSI White Paper No. 3
Interoperability (Semantic)	Usually associated with the meaning of content and concerns the human rather than machine interpretation of the content. Thus, interoperability on this level means that there is a common understanding between people of the meaning of the content (information) being exchanged	ETSI White Paper No. 3
Interoperability (Organizational)	Ability of organizations to effectively communicate and transfer (meaningful) data (information) even though they may be using a variety of different information systems over widely different infrastructures, possibly across different	ETSI White Paper No. 3

	geographic regions and cultures. Organizational interoperability depends on successful technical, syntactical and semantic interoperability.	
Mandate	Political request from the European Commission (EC) (and European Free Trade Association (EFTA)), agreed upon by the Member States (generally via a decision of the Standing Committee of the Directive 98/34), addressed to CEN, in support of an action from the EC. This can be in support of legislative work such as a directive (some directives, not all, are 'New Approach' Directives), or in support of an industrial policy action from the EC.	
Regulation	Document providing binding legislative rules, that is adopted by an authority	ISO/IEC 17000:2004
Standard	Document, established by consensus and approved by a recognised body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context	ISO/IEC 17000:2004

1 Introduction

1.1 Context FI-PPP

With over a billion users world-wide, the Internet is one of history's great success stories. Its global, integrated communications infrastructures and service platforms underpin the fabric of the European economy and society. Yet today's Internet was designed in the 1970s, for purposes that bear little resemblance to current and future usage scenarios. Mismatches between the original design goals and how the Internet is being used are beginning to hamper its potential. Many challenges in the areas of technology, business, society and governance will have to be overcome if the future development of the Internet is to sustain the networked society of tomorrow.

To answer these challenges, the European Commission has launched the Future Internet Public-Private Partnership Programme (FI-PPP). The main goal is to advance a shared vision for harmonised European-scale technology platforms and their implementation, as well as the integration and harmonisation of the relevant policy, legal, political and regulatory frameworks. As set forth in the Digital Agenda for Europe, these are considered to be prerequisites for realizing a European online Digital Single Market (DSM) and, more broadly, an inclusive knowledge society.

Programme aims are to:

- Increase the effectiveness of business processes and infrastructures supporting applications in areas such as transport, health, and energy.
- Derive innovative business models that strengthen the competitive position of European industry in sectors such as telecommunication, mobile devices, software and services, and content provision and media.

Programme approach:

The FI-PPP follows an industry-driven, holistic approach encompassing R&D on network and communication infrastructures, devices, software, service and media technologies;

In parallel, it promotes their experimentation and validation in real application contexts, bringing together demand and supply and involving users early in the research lifecycle.

The new platform will thus be used by a range actors, in particular SMEs and Public Administrations, to validate the technologies in the context of smart applications and their ability to support «user driven» innovation schemes.

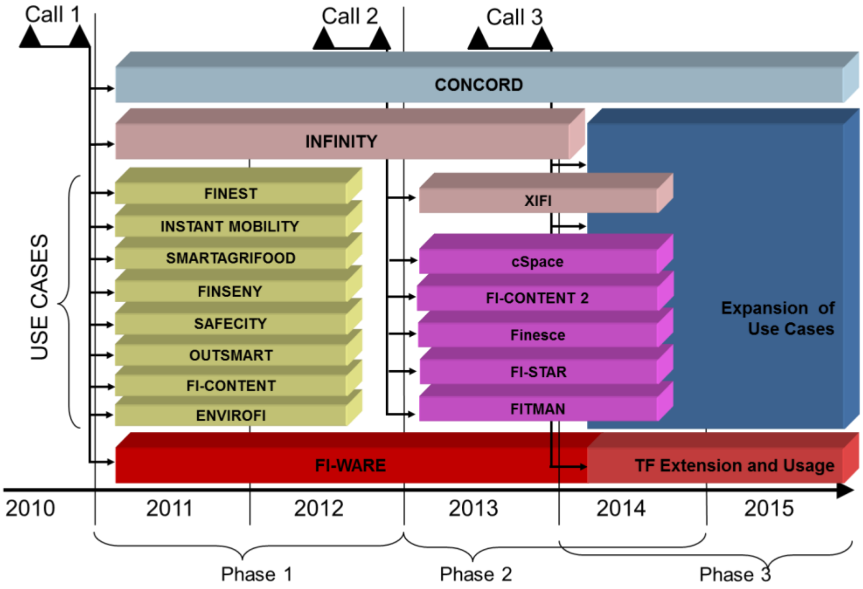


Figure 1: FI-PPP program

The participation of actors including *SMEs and Public Administrations, to validate the technologies* will lead to involve much more actors to use the platform components and therefore will raise a lot of new issues related to support these new stake holders in using the FI-PPP components. **Confidence in the whole programme will be at stake and can be easily endanger if too much weaknesses would be detected**. Information on difficulties to use the platform or weaknesses in technical elements uses to be quickly spread up by communities. To prepare such important taking up by larger communities, **it is important to develop programme to reinforce the robustness of the technical elements while giving reasonable level of confidence to users**. This kind of activities are main part of certification or label scheme and such concept was raised at FI-PPP level in particular when FI-STAR made clear on its firm intention for its own project to ensure robustness of its development and to give confidence to end users by certification.

In such new expectation from the FI-PPP programme, FI-STAR is invited to provide input to "certification" where good practices might be extended to the whole programme. As a part of FI-STAR , but not only, will be dedicated to check conformity to GEs, it is likely feasible that FI-STAR tests and tools could be used for the FI-PPP programme.

EC made also clear that, while FI-STAR is operating in the eHealth domain, one of its important objectives is, through the eHealth demonstrators and pilots, is to support and validate the whole programme. Such statement made clear to FI-STAR partner that looking at certification requirements means paying a large attention to certification supporting the FI-PPP programme. Therefore high attention will be devoted to FI-PPP while some extend will still be kept to deal with important eHealth certification issues.

1.2 Overall objectives of Standardisation and Certification for FI-STAR

This document is looking at Standardisation and Certification requirements. A lot of activities where already undertaken on Standardisation and Certification in the eHealth sector. Following chapter will present a lot of existing activities in Certification and Standardisation that FI-STAR is aware of. Some activities exist also in the FI-PPP context as also FI-STAR is member of the FI-PPP Standardisation WG. Therefore out study where focussing on what are the added values that FI-STAR can provide to existing studies and what are the topics important for FI-STAR to deliver its services and subsequently what would be therefore the requirements.

As this will presented here below, the overall conclusion of our analysis is that

- As far are **Standardisation** requirements concerned, FI-STAR will pay more attention to the **eHealth domain** as general standardisation is treated at the FI-PPP level. A lot of guidelines are already identified in eHealth area from which FI-STAR can benefit.
- As far as **Certification** requirements are concerned, FI-STAR will pay more attention to the **FI-PPP domain** as nothing is really implemented within the programme while many activities in certification exist in eHealth and other many certifications solution are available on the market (e.g. ISO80000) or by European projects (e.g. HITCH, ANTILOPE) assuming FI-STAR implement standardisation guidelines (e.g. certification to existing profile)

1.2.1 Objective of Standardisation requirements (eHealth oriented)

As a lot of projects and European studies have worked on standardisation (see section 2.1), the main work of FI-STAR in D2.1 is to identify the health standards relevant for the project and to be transferred into requirements as well as to identify the areas where FI-STAR contribution would make sense. These include:

1. Overall interoperability issues in particular at the semantic (data and content/meaning) level
2. Support validation and certification with implementation done in WP6
3. Work smoothly with the technical platforms, with WP6 support and FI-WG on standardisation

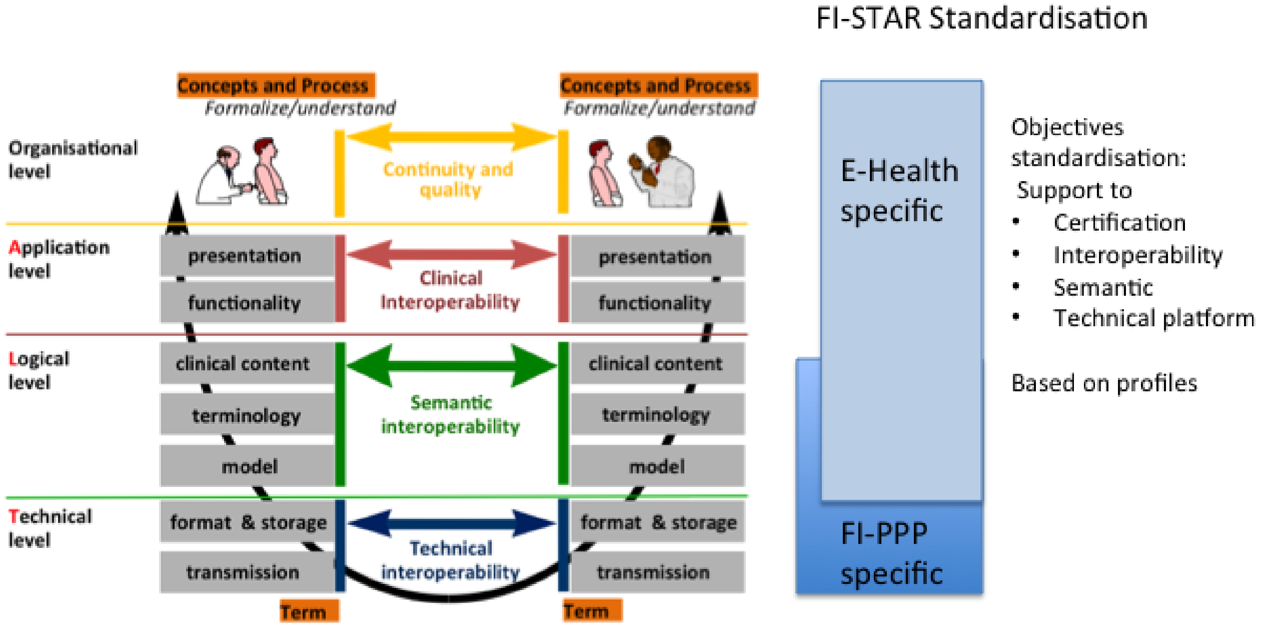


Figure 2: ALT model modified (from HITCH project [2])

To reuse very important work from previous and current projects (Figure 3), **it is important for FI-STAR to study whether FI-STAR implementations can be compatible with eHealth profiles as a lot of guidelines, tests and certification tools exist**.

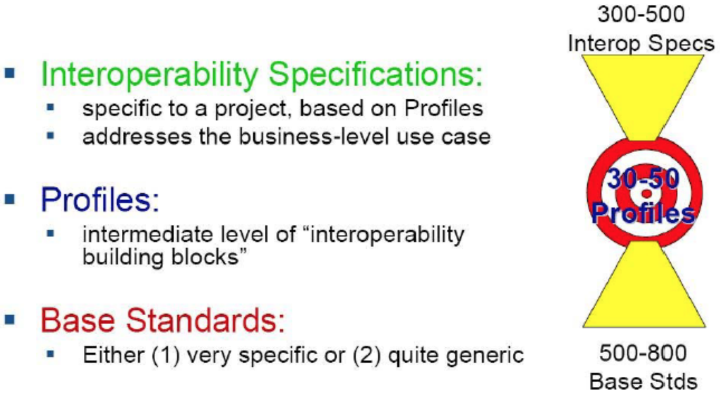

Interoperability Specifications:
specific to a project, based on Profiles
addresses the business-level use case
Profiles:
intermediate level of "interoperability building blocks"
Base Standards:
Either (1) very specific or (2) quite generic
300-500 Interop Specs
30-50 Profiles
500-800 Base Stds

Figure 3: importance to capitalize on profiles (source European Commission Mandate M403:2007 [3])

The process followed in this document to identify requirements goes through the identification of the relevant profiles for FI-STAR, based on the FI-STAR use cases.

1.2.2 Objective of certification requirements (FI-PPP oriented)

Certification is a very large concept (see also section 3) so we have to define the objectives of the certification approach to be in line with FI-STAR interest which are to:

1. Ensure **regulatory compliance** ISO 80001 (security for health system), privacy, local regulations) & EN27000
2. Ensure **internal quality** of the development to be sure that what is developed is according to FI-STAR requirements best practices. This is ensure by Verification and Validation approaches (V&V), Quality of services checking and Quality of Experience as measure by users (See WP6)

3. Ensure FI-PPP plugability, interchangeability and interoperability[1]. This can be ensure by checking conformity to FI-PPP specifications and interfaces (See WP6)

In FI-STAR we will therefore identify 4 processes to be fulfilled before getting a complete certification scheme (more details are given in section 3). As refined within the FI-STAR quality assessment framework (WP6), which identify the indicators as well as the tools and processes to collect and analyse them, the 4 processes are (Figure 4):

1. Define quality objectives within the quality assessment framework.
2. Define eHealth certification scheme when relevant as such certification is expected to be mainly sought independently from the FI-STAR project, depending on each use case exploitations plan. Indeed, many relevant health certification schemes are available on the market or made available by other projects (e.g. Antilope) and focus should rather be made on FI-STAR specific eHealth profile certification if required.
3. Define GE or SE conformity objectives as made available by FI-STAR GE/SE tests and tools
4. Set GE, SE and FI-STAR applications Verification & Validation (V&V) processes as available by Fi-STAR and can use if necessary FI-STAR test bed or external test bed (ex FI-LAB, FI-OIL or XIFI test beds).

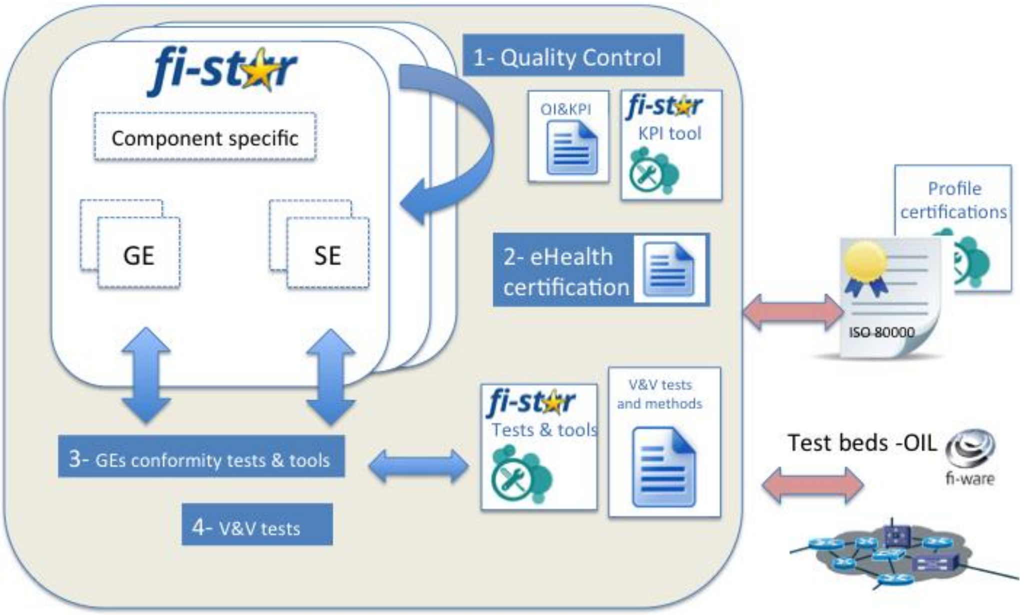


Figure 4: FI-STAR proposed certification points

Such FI-STAR certification for a FI-STAR component can be used with a full chain of Quality and Validation approach. While the certified product can be placed on the market and available for instance in a FI-STAR app store; Such certification tools can also be used also to check quality on the market as illustrated in the Figure 5.

[1] Plugeability and interchangeability: here define the ability to be "plugged" in any FI-PPP environment offering the requested GE or set of GEs. The danger is to have an application checked in one environment that could not work in another environment. Interoperability here mean capability of two components implementing the same specification, to work together.

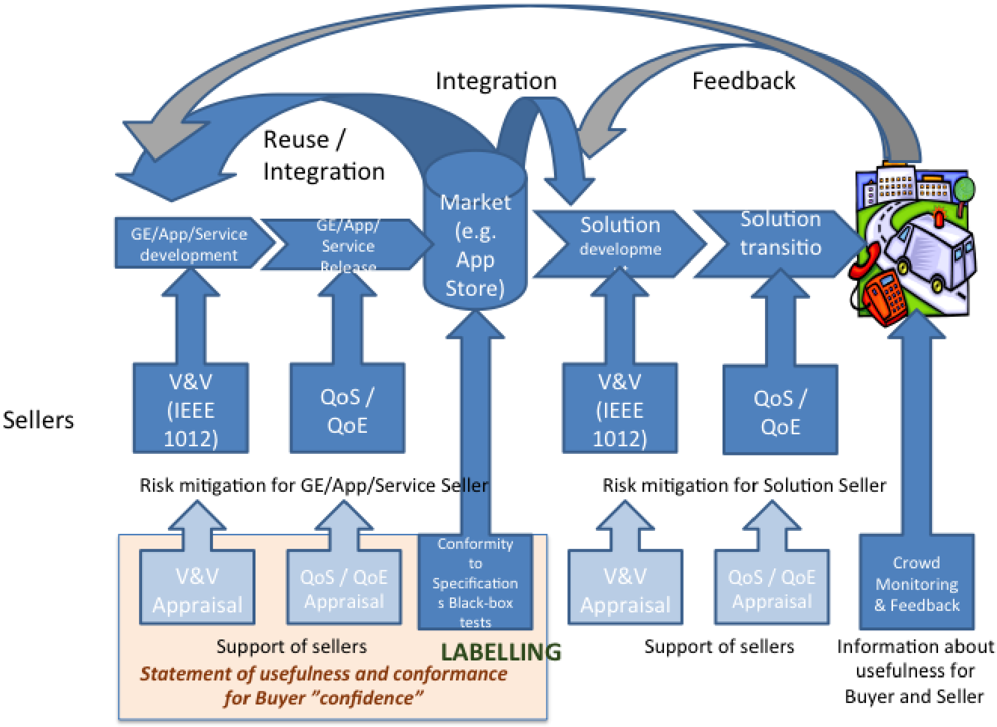

Integration
Feedback
Reuse / Integration
GE/App/Service development
GE/App/ Service Release
Market (e.g. App Store)
Solution developme
Solution transitio
Sellers
V&V (IEEE 1012)
QoS / QoE
V&V (IEEE 1012)
QoS / QoE
Risk mitigation for GE/App/Service Seller
Risk mitigation for Solution Seller
V&V Appraisal
QoS / QoE Appraisal
Conformity to Specifications Black-box tests
V&V Appraisal
QoS / QoE Appraisal
Crowd Monitoring & Feedback
Support of sellers
LABELLING
Statement of usefulness and conformance for Buyer "confidence"
Support of sellers
Information about usefulness for Buyer and Seller

Figure 5: positioning certification points over the value chain.

2 Standardisation requirements

2.1 Introduction: interoperability requirements

With the development of the ICT in Health in many medical specialties as well as in public health and patient access to his medical information, eHealth standards become the key for the success of the deployment of these technologies. This is why the European Commission set up the digital agenda for Europe and action plan 2012-2020 in eHealth that the purpose is to consolidate the actions that have been taken in the previous action plan started in 2004. Four objectives were defined and the objective 2 is to “address issues currently impeding eHealth interoperability” by achieving wider interoperability in eHealth services. The need of an eHealth European Interoperability Framework was one of the listed covering technical and semantic levels among the four levels of interoperability that were also targeted.

Before reaching this major step, the EU Commission “has issued a mandate to the European Standardizations organisations CEN, CENELEC and ETSI to develop a coordinated work program for standardization in health informatics” called Mandate M/403 [3]. The background was already well established and the following schema synthetizes all the aspects of the standardisation taken into account regulation, organisational and functional, technical and semantic layers.

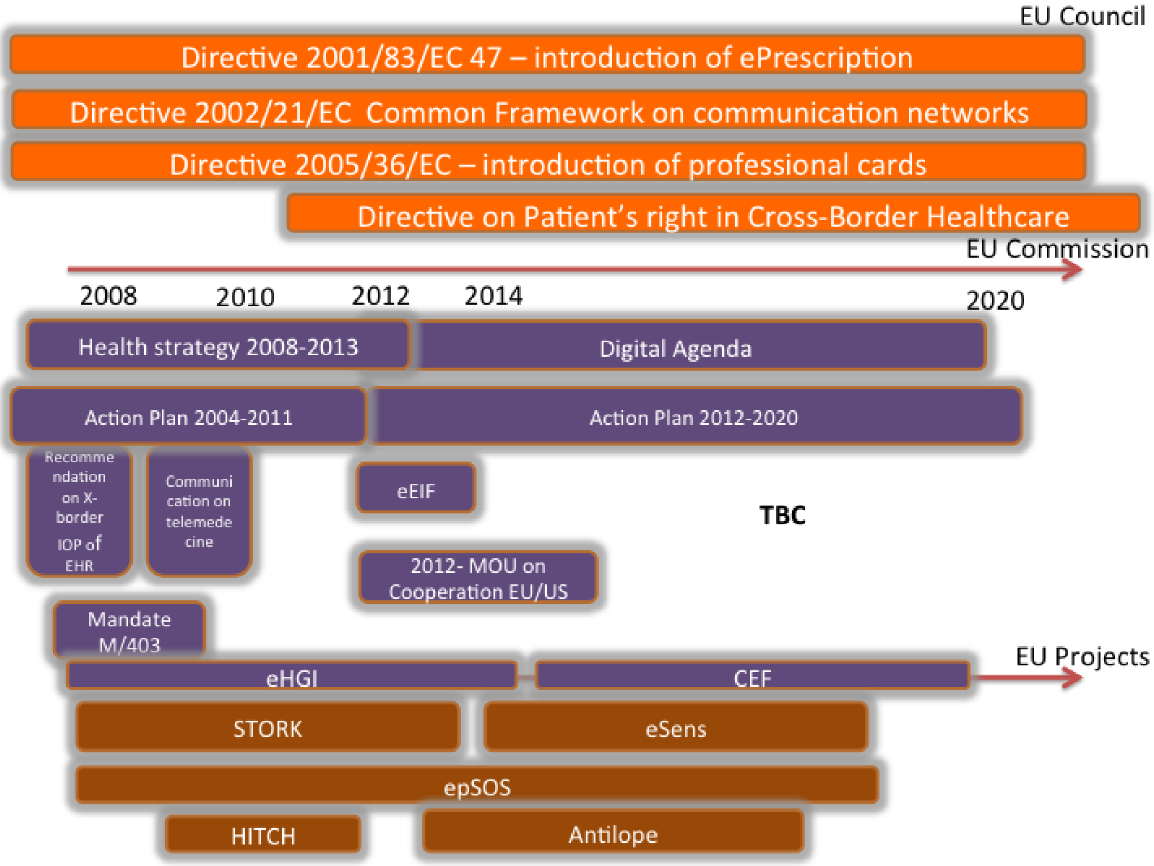

EU Council
Directive 2001/83/EC 47 – introduction of ePrescription
Directive 2002/21/EC Common Framework on communication networks
Directive 2005/36/EC – introduction of professional cards
Directive on Patient’s right in Cross-Border Healthcare
EU Commission
2008
2010
2012
2014
2020
Health strategy 2008-2013
Digital Agenda
Action Plan 2004-2011
Action Plan 2012-2020
Recommendation on X-border IOP of EHR
Communication on telemedecine
eEIF
TBC
2012- MOU on Cooperation EU/US
Mandate M/403
eHGI
CEF
EU Projects
STORK
eSens
epSOS
HITCH
Antilope

Figure 6: European Interoperability Environment

The levels of interoperability can also be represented within a healthcare process represented in the Figure 7.

To ensure **clinical interoperability** in which healthcare providers are able to exchange clinical information within business processes, the concepts, and the activities must be correctly interpreted and the meaning safe. It means that at each level of the description of the concepts and its treatment has to be correctly transformed using common “interpreters” at each level. **Semantic interoperability** is one of the key of the interoperability exchange and the more difficult level to achieve.

Technical interoperability (sometime completed with syntactical interoperability as in the ETSI four layers interoperability model [4]) is the prerequisite of the semantic interoperability. This layer ensures that appropriate protocols are in place to enable machine to machine communications (technical level) and that data can be exchanged (syntactical level). Definition of data structure, communication and protocols is the condition for processing and exchanging data and is the basis of the standards and profiles.

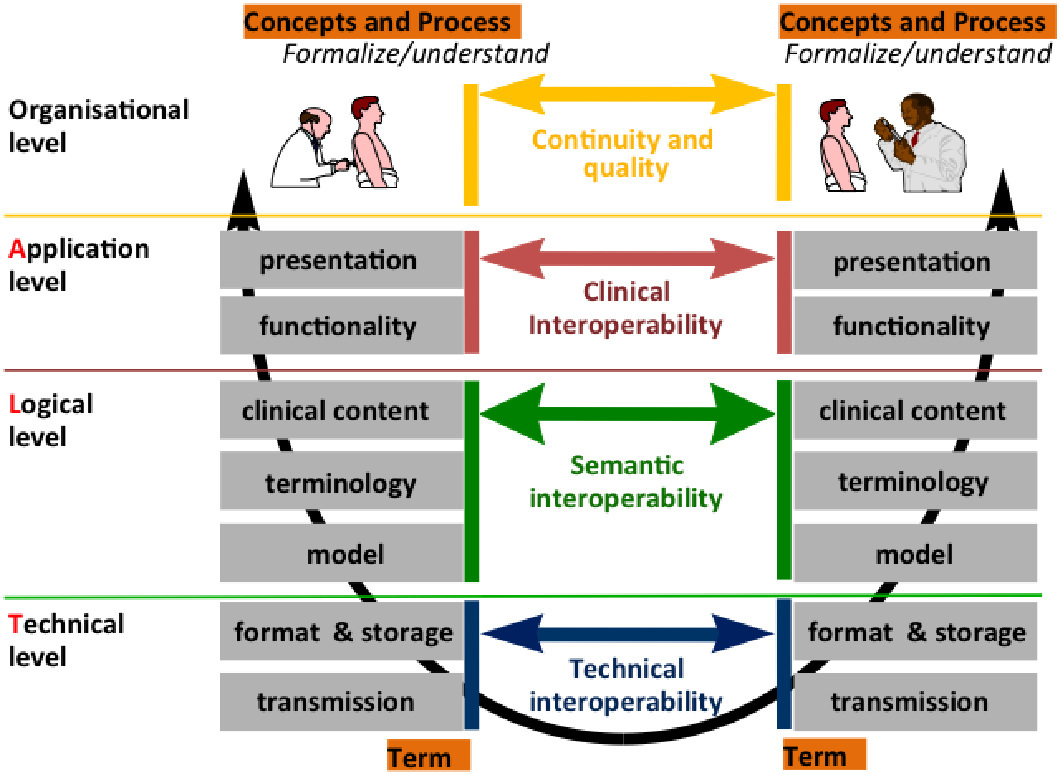


Figure 7: derivation from ALT model

Several European projects have been promoting standards and certification in eHealth during the last past years. Without idea of completeness, the following projects emphasize the interest of the usages of standards in eHealth. Quality assurance and certification of the EHR systems was one of the topics of the EHRQTN project [8]. The aim was to promote the certification products by validating the functional statements translating a substantial set of them in over 20 different European languages. These functional statements are based on European and International standards such as HL7 Electronic Health Record System functional model.

The HITCH project was focused on Interoperability labelling or certification and testing process [2]. The main purpose was to give an overview on the state of Art in term of testing tools and certification/quality labelling organised by entities, consortia and countries in Europe, to define the interoperability quality management system and its application on testing processes, and define a two level interoperability quality label or certification process. The Antilope project, started in February 2013 is the follow-up with an additional item on eHealth European Interoperability Framework based on epSOS use cases, national/regional use cases, IHE profiles and Continua alliance guidelines for the homecare use cases.

Quality assurance for EHR systems based on EHR standards, has positive impact by improving liability of vendor (decreasing the number of vendors), the development of software by enhancing the functionalities and facilitating the medical practises of the Healthcare professionals by a better support of the regulation and finally diminishing the cost of a treatment keeping up the same level of quality.

The impact of having an eHealth European Interoperability framework is also positive by increasing a common view of healthcare architectural services that can be directly used by national/regional programs based on similar use cases that are developed in the Interoperability Framework. Using certified services allow the development of reliable communication in the field of medical sharing or exchanging data between Healthcare Professionals, Patient and Public Health by transmitting public reporting.

2.2 Standardisation within FI-PPP programme

2.2.1 FIWARE Standardisation Plan

The standardisation within the FI-PPP programme is mainly based on issues related to GEs which are provided by FIWARE, the Core Platform project.

On the available FIWARE information related to standardisation plan we can read*: FI-WARE Project studies the actual standards and consider when/how to contribute FI-WARE research into new standards/protocols in order to (a) avoid "re-inventing the wheel", (b) make the most efficient use of past developments, and (c) help educate/move technology state-of-the-art towards the advantages inherent in FI-WARE. Its Standardization Plan describes the status of the relevant parts of the global standardization landscape, and plans related to FI-WARE activities. It is a "living document" which will be updated as work progresses during the life of the project. The high-level goal of the FI-WARE project is to build the Core Platform of the Future Internet. This Core Platform, also referred to as the "FI-WARE Platform" or simply "FI-WARE", has been proposed as an innovative infrastructure for cost-effective creation and delivery of versatile digital services, providing high QoS and security guarantees. A basic description is available publicly in our FI-WARE Product Vision.*

To understand the broad range of topics covered, it is sufficient to note that the Core Platform provided by the FI-WARE project is based on enabler functions linked to the following main architectural areas:

- **Service Delivery Framework** – the infrastructure to create, publish, manage and consume FI services across their life cycle, addressing all technical and business aspects.
- **Cloud Hosting** – the fundamental layer which provides the computation, storage and network resources, upon which services are provisioned and managed.
- **Data/Context Management Services** – the facilities for effective accessing, processing, and analysing massive streams of data, and semantically classifying them into valuable knowledge.
- **IoT Enablement** – the bridge whereby FI-WARE services interface and leverage the ubiquity of heterogeneous, resource-constrained devices in the Internet of Things.
- **Interface to the Network and Devices** – open interfaces to networks and devices, providing the connectivity needs of services delivered across the platform.
- **Security** – the mechanisms which ensure that the delivery and usage of services is trustworthy and meets security and privacy requirements.

The set of strategic goals of the FI-WARE project are:

- To specify, design, and develop a Core Platform ("FI-WARE") to be a generic, flexible, trustworthy and scalable foundation, supporting the equations listed previously.
- Design extension mechanisms so as to enable to support for yet unforeseen Usage Areas not being addressed in the context of the FI-PPP. This requires a suitable extrapolation of current technology and business trends and their translation into the specific design and implementation principles of FI-WARE.
- To liaise between the project and relevant standardization bodies in order to: a) to keep the project up-to-date with respect to the discussions in the standardization bodies; b) to support the submission of contributions from the project in a coordinated way. The aim is to ensure active contribution of specifications leading to open standardized interfaces.
- To implement and validate the FI-WARE approach in trials together with Use Case projects in order to develop confidence for large scale investments in solutions for smart future infrastructures on national and European level.

- To enable established players (telecoms, etc.) and emerging players in the services and application domains to tap into new business models by providing components, services, and platforms for these emerging players to innovate.
- To support the development of a new ecosystem including agile and innovative service providers consuming components and services from FI-WARE thereby building new business models based on FI-WARE and associated Usage Areas.
- To stimulate early market take-up by promoting project results jointly with the other projects in the FI-PPP.

A specific activity "Exploitation and Standardization" is dedicated to co-ordinating and reporting the standardization work done within FI-WARE. The remaining of the Standardization Plan is divided into sections as follows:

a) Standardisation needs
    - Survey the SDO landscape
    - Identify relevant SDOs for each work area, (especially the architectural and technical topics)
    - Classify SDOs into "Will Monitor“, "Will Use", "Will Contribute“
b) Standardisation gaps analysis [6]
    - For each interface, and for each GE, analyse which standard (or open source specification or consortia specification or published Web API, etc.) is relevant and what are the gaps in functionality between the existing status and what is needed within FI-WARE
    - Create action items within each technical area, designed to fill those gaps, by adapting/creating standards to be "fit for purpose" within FI-WARE
c) Strategy for standardisation for Technical area

The goal of this section is to define a strategy for each one of the technical chapters by assigning the action items needed in each SDO to specific partners, taking account of existing partner resources within various SDOs.

Based on discussions between experts within each SDO, the action items will be organized into a timetable matching the pace of step-by-step development of functionalities within FI-WARE R&D and the pace of meetings of each SDO.

At the time of writing the first version of this report, only general plans can so far be presented.

2.2.1.1 Contribution to FI-PPP Standardisation plan

FI-STAR is member of the FI-PPP Standardisation working group. Activities in standardisation did not appear having important item to address because most of standardisation look to be treated outside the FI-PPP communities by members being active in various Standards Developing Organisation (SDO).

FI-STAR has however detected a need for complementary “standards” related to testing and validation. FI-STAR representative has therefore initiated a discussion within FI-PPP community to extend the Standardisation WG by Standardisation and Validation Working group. Presentation were made at the FI-PPP Architecture board in December 2013 in Madrid and decision to address validation also impacting standards is expected by the FI-PPP AB in January 2014

Text of the suggested Term of Reference is given in annex. Extract of the text:

Standardisation & Validation working group

The main objective of the Standardisation and Validation Work Group (WG) is to facilitate the projects in the identification of existing and potentially applicable standards and in the process of standards definition from pre-standardisation to compliance testing and marketing, and help maximise the outcome of the Future Internet PPP. A first goal of this WG is to provide advice about existing standards that can be used in a FI-PPP project, when the project requires it. Another objective is to ensure that projects and developments are correctly implementing existing standards and that new standards can be validated wherever feasible. Standards aim to ensure *interoperability and such goal can be achieved only if there is clear identification of conformity to standards process we called here "validation"*

2.3 eHealth specific standardisation

2.3.1 Background, Motivation, and Approach

In the healthcare industry, standards and regulations are frequently perceived as limitations or hurdles, which need to be overcome in order to establish trust in new technologies. Some of these regulations are global, while others are applicable just for some types of systems and regions. Although especially with regards to health and safety reasons the necessity of standards and regulation is undisputed, regulations on the other hand make product development risky and costly, hence discourages software and electronic companies to contribute to value creation and innovation.

Software ecosystems, such as the "Fi-WARE Core Platform" and its modular design consisting of a variety of GEs provide an opportunity to reduce this hurdle for software product companies. Interfaces, data models, and protocols can be integrated into enabling components ready for use by application developers. Application stores are able to embed rules for assuring compliance and provide certification mechanisms. Such hiding of regulatory rules and procedures allows software companies to focus on value creation for the customer and on differentiation towards competitors, while benefiting from central services to learn how to address regulation and to check application compliance.

The first step in the design of such support is a mapping of relevant standards and regulations. The map enables identification of responsibilities, services, and rules that are to be delivered by the software ecosystem. Such support will reduce cost and risk of new software development and offer more consistent level of compliance across software products.

This section gives an overview of standards that are applicable for the healthcare, wellness and ambient assisted living sectors and outlines the implications of these standards on ecosystem design. Enabling such transparency regarding which standards are applicable allows generating a debate on the scope of regulations to be considered, creates the fundament for implementation of the ecosystem, and provides a baseline for road-mapping how standardization should evolve.

To identify the here presented standards, we have selected two different solutions conceived by healthcare providers and have elicited their needs for compliance. Furthermore relevant standards have been identified in the literature. Included here are the standards of relevance for software products to be used in health care, wellness and ambient assisted living environments comprising of software products, professional users such as nurses and doctors, and the general public such as patients and caregivers. **Overall, the presented standards apply to infrastructures, which are generally referred to as "medical data networks". Excluded were standards that relate to the design and construction of physical equipment only. Also excluded were national regulations and standards under development.**

2.3.2 Overview of Standards

Analysis of standards showed five groups of standardized aspects:

1. Development of a software product,
2. Interoperability of the product with other products,
3. Usage of the product by a human user,
4. Resilience to protect from harm, and
5. Data security

These five groups of regulated aspects **assure good-enough quality for the software to be used in a mission-critical care environment as well as appropriate data management**. The remainder of the section gives an overview of the four regulated aspects of a software product intended for care.

The standards focused on are typically regulating one aspect at a time. However, in practice the boundaries are blurred. For example, the technical aspects of interoperability affect the human aspects of perceived usability [24]. Also, as indicated in ISO/TR 16982, usability affects not only the design, but also the process used to develop the software product and trust in the released software product.

Software Development: IEC 62304 regulates the development of software for medical devices. It adds the aspects of risk and quality management to the established good practices suggested by frameworks like CMMI and ITIL and development lifecycle models such as waterfall and agile. It constrains development, maintenance, risk management, configuration management, and problem resolution practices based on an assessment of safety criticality of the software. IEC 62304 compliance contributes to FDA [25] compliance.

ISO 9241-210 specifies the processes of designing interactive systems from a usability perspective, and ISO/TR 16982 specifies the use of usability engineering methods as part of such development processes. IEC 62366 defines the corresponding process to be followed for engineering medical devices.

Further guidance for software development can be obtained by other IEEE and ISO/IEC standards, which are applicable for software engineering in general and not for healthcare, wellness, and ambient assisted living in particular. Standards of relevance are the IEEE Standard Glossary of Software Engineering Terminology 610.12 and ISO/IEC 25010 for Systems and Software Quality Requirements and Evaluation.

Interoperability: A software product embedded in a solution has to communicate with other software products and medical devices. To enable independence from the manufacturer of these products, ISO/IEEE 11073 specifies how the products interact. It is a family of standards that defines the application domain, terms, information model, types of devices, applications, data transport, and data encoding. ETSI ES 202 975, even-though not specific for the health domain, further constrains communication of text, speech, and video in a network.

Information that is of particular relevance in the care sector is the patient profile. CEN/TC 251 has developed a collection of standards on health informatics for health interoperability. CEN/ISO 13606 is of particular importance as it specifies electronic health record communication. It captures a reference model that allows the formulation and aggregation of statements of relevance for the health record, an archetype model that defines health concepts and their meaning, and allows defining data protection rules that govern the access to the data the health record contains. ISO/TS 19218 specifies coding practices for describing adverse events relating to medical devices. ISO 15225 defines a medical device nomenclature data structure for exchange of data used by regulatory bodies.

Usability: Much work was invested in standardizing the interaction between humans and software-based systems with the goal of simplifying the interaction between users and software and of enabling effective support of these users. The multi-part standard ISO 9241 defines the design of input and output devices that allow users to interact with software-based systems, the interaction process, and the physical context such as the workplace in which users interact with the systems.

Software user interfaces are used to present a wide variety of functionality and information to users. The multi-part standard ISO 14915 establishes design principles for the interaction of professional users with text, graphics, audio, animations, video, and media related to other sensory modalities. IEC TR 61997 defines guidelines for multimedia interfaces that are used by the general public without any special previous training. ISO 15223 defines symbols and the development of such symbols to be used to convey information on the safe and effective use of medical devices.

Safety, Resilience and Trust: A new software product may not only produce new value, but also destroy or endanger existing value. The new product may harm people or existing processes or generate fear of such harm. ISO/TR 16142 provides guidance on the selection of safety and performance- related standards for medical devices that allow establishing trust that the new product will not produce harm.

IEC 80001 specifies the perspective of the care provider by defining how to manage safety, effectiveness, and security of an integrated healthcare system. It defines roles and responsibilities, and risk management policies and processes for medical IT networks and for enhancement and change of these networks. The ISO 27000 family of standards establishes vocabulary, requirements, and processes for managing security and security-related risks of such integrated systems. In particular:

- ISO/IEC 27001:2013 “Information technology -- Security techniques -- Information security management systems – Requirements”[2] contains information security requirements generic for all types of organisations. It contains “the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization,” as well as for “the assessment and treatment of information security risks.”
- ISO/IEC 27002:2013 is complementary to ISO/IEC 27001:2013 and contains guidelines for organizational information security standards and information security management practices, “taking into consideration the organization's information security risk environment(s).”
- Standard ISO 27799:2008 contains guidelines on best practices and indicators of health data security. It supports the interpretation and implementation in health informatics of ISO/IEC 27002 and is complementary to that standard.

The product supplier perspective is covered by ISO 14971 that IEC 80001 now integrates. ISO 14971 specifies the risk management practices to be followed by a medical device manufacturer. ISO 13485 defines regulatory requirements for medical devices, including documentation, management, product realization, and quality assurance processes. IEC 60601 standardizes safety practices for medical electrical equipment.

Data security: Current data protection legislation does not contain mandatory requirements to comply with particular data security standards or of data security certification. However, using such standards contributes to establishing whether or not the data controller abides by the data security obligations under the DPD.

Under Article 17 DPD, the data controller has an obligation to take – and make sure that the processor acting on his behalf takes - both organizational and technical measures [10] to ensure the adequate protection of personal data from any kind of unauthorised processing, such as destruction, alteration, disclosure and loss, both at the stage of designing data processing processes and during the processing itself (Recital 46 DPD).

The Directive uses an *objective standard of quality* of security measures. It means that the measures must be in proportion to the risks involved in the data processing and ‘the state of art and the cost of their implementation’ (Article 17(1)). The reference to ‘the state of art’ of security measures establishes a clear link between the legal requirement of data security and security standards.

ENISA reports that, although currently using specific data security standards is legally not required, ‘legal precedents may emerge, particularly in common law jurisdictions, when defendants are given 'credit' for being certified’ [11].

The recently published Cybersecurity Strategy of the European Union [12] states the need to develop industrial and technical resources for cybersecurity. Among the actions it is mentioned that “prime focus should be to create incentives to carry out appropriate risk management and adopt security standards and solutions, as well as possibly establish voluntary EU-wide certification schemes building on existing schemes in the EU and internationally” [3]. FI-STAR will be following up the developments in this area and will encompass any outcome relevant to the project.

The next table provides the synthetic list of previously listed standards

[2] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

[3] ibid, p. 12.

Table 1: standards relevant for FI-STAR

Reference	Title
Software	
ISO/TR 16982[4]	Ergonomics of human-system interaction -- Usability methods supporting human-centred design
IEC 62304	Medical device software - Software life cycle processes
ISO 9241-210	Ergonomics of human-system interaction -- Part 210: Human-centred design for interactive systems
IEC 62366	Medical devices -- Application of usability engineering to medical devices
Interoperability	
ISO/IEEE 11073	Family of standards for health device communications.
ETSI ES 202 975	Human Factors (HF); Harmonized relay services
CEN/TC 251	Collection of standards on health informatics for health interoperability
CEN/ISO 13606[5,6]	Health informatics -- Electronic health record communication (5 parts) • Part 1: Reference model • Part 2: Archetype interchange specification • Part 3: Reference archetypes and term lists • Part 4: Security • Part 5: Interface specification
ISO/TS 19218[7]	Medical devices -- Hierarchical coding structure for adverse events (2 parts) • Part 1: Event-type codes • Part 2: Evaluation codes
ISO 15225:2010[8]	Medical devices -- Quality management -- Medical device nomenclature data structure
Usability	
ISO 14915[9]	Software ergonomics for multimedia user interfaces (3 parts) • Part 1: Design principles and framework • Part 2: Multimedia navigation and control • Part 3: Media selection and combination

[4] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=31176

[5] http://www.en13606.org/

[6] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=40784

[7] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=55589&commid=54892

[8] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50728

[9] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=25578&commid=53372

IEC/TR 61997[10]	Guidelines for the user interface in multimedia equipment for general purpose use
ISO 15223[11]	Medical devices -- Symbols to be used with medical device labels, labelling and information to be supplied (2 parts) • Part 1: General requirements • Part 2: Symbol development, selection and validation
Safety, resilience and trust	
ISO/TR 16142	Medical devices -- Guidance on the selection of standards in support of recognized essential principles of safety and performance of medical devices
IEC 80001[12]	Application of risk management for IT-networks incorporating medical devices (5 parts) • Part 1: Roles, responsibilities and activities • Part 2-1: Step by Step Risk Management of Medical IT-Networks; Practical Applications and Examples • Part 2-2: Guidance for the communication of medical device security needs, risks and controls • Part 2-3: Guidance for wireless networks • Part 2-4: General implementation guidance for Healthcare Delivery Organizations
ISO 27000[13]	ISO/IEC 27000:2009 provides an overview of information security management systems. In particular: • ISO/IEC 27001:2013[14] "Information technology -- Security techniques – Information security management systems – Requirements" • ISO/IEC 27002:2013[15]: "Information technology -- Security techniques – Code of practice for information security controls" • ISO 27799:2008[16]: "Health informatics – Information security management in health using ISO/IEC 27002"
ISO14971[17]	Medical devices – Application of risk management to medical devices
ISO 13485[18]	Medical devices -- Quality management systems -- Requirements for regulatory purposes
IEC 60601	Medical electrical equipment. Several parts

[10] http://webstore.iec.ch/Webstore/webstore.nsf/ArtNum_PK/27914!opendocument

[11] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50335

[12] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44863&commid=54960

[13] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=41933

[14] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

[15] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533

[16] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=41298

[17] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=38193

[18] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=36786

2.3.3 Impact of the Standards

The presented standards are embodied in many national regulations, are common practice of experienced software product suppliers, and are part of awarding the CE label for products intended for the care sector. This is also important for compliance with the Medical Devices Directive [27]. To help new software products to reduce cost and risk associated with compliance, the provided overview of standards represents a starting point to identify roles, responsibilities, and services in a compliance-enabling software ecosystem.

2.3.4 Discussion

This chapter gives an overview of relevant norms and standards for the development and instantiation of technologies in the health care, wellness and ambient assisted living domains and the implementation of medical data networks. Special consideration has been given to governance requirements expressed through legal and technical norms and standards on the interface of the "FI-WARE Core Platform" which is also known as the Generic Enabler concept and the "Internet of Things". Technical standards have been named and highlighted in this paper. Citations of text elements of technical standards or the cross reference to "full texts" are generally not possible as definitions of the standards are typically not in the public domain and copyright protected. Full versions of these standards may be purchased for further reading.

Legal norms and ethical considerations have been discussed with focus on the relevance to the healthcare, wellness and ambient assisted living domains. Due to the magnitude of the subject it was not possible to cover national legislation for the different European member states. US standards such as those published by HIPAA (Health Insurance Portability and Accountability Act of 1996) and overseen by the US Department of Health and Human Services and rules and regulations established and overseen by the FDA (Food and Drug Administration) have not been considered in the context of this paper. It should be mentioned that in recent years the medical product regulations in many countries have been extended and do now cover software products, as well as hardware, which has not always and everywhere been the case. This means that typically software has to comply in full with national medical product legislation.

There is good evidence that future "medical" architectures will be modular and follow European wide defined specifications. **Health care providers have rejected public e-health cloud approaches in Europe and elsewhere and single standing solutions are unlikely to continue due to regulations and cost aspects**. There has been good progress fuelled by EC funded research with regards to the cross border transfer of medical data sets within Europe [28]. Our future work under FI-STAR will include a mapping of the standards discussed in this paper onto Generic Enablers and Usage Specific Enablers. As part of our progressive work we will also map those standards, which so far could not be considered, such as the US standards and legislation in different European national states.

Another important part of our work will be to look into commercial distribution strategies and business models in order to establish application distribution platforms (app-stores).

The technical targets of FI-STAR will be the validation of domain relevant Generic Enablers and Usage Specific Enablers in the healthcare, wellness and ambient assisted living domain.

2.4 Requirements and recommendations

2.4.1 FI-STAR profiles and standards mapping

Profiles are generally defined for the integration purpose. Profiles provide to developers a clear implementation path for communication standards, carefully documented, reviewed and tested. Profiles reduce the complexity of the implementation of the communication functions or use cases by specifying a subset of standards that limit and precise their usage for the specific needs. Profiles are standards-based choices in different levels such as application interfaces, protocols for communication, security level, file format, and semantic.

2.4.1.1 Example: the epSOS Project

The objective of the epSOS project is to exchange medical data of the mobile patient between healthcare professionals (HP) from the source (called country A, where the patient is originated) to the HP of the visiting country (called country B) in a secure environment. The medical data are

- The patient Summary
- The eMedication including the ePrescription and the eDispensation

The selected architecture is based on a NCP (National Contact Point) and the epSOS provides epSOS services based on IHE profiles. The terminology is provided by the central services as well as configuration and traceability services and other common services (see Figure 8).

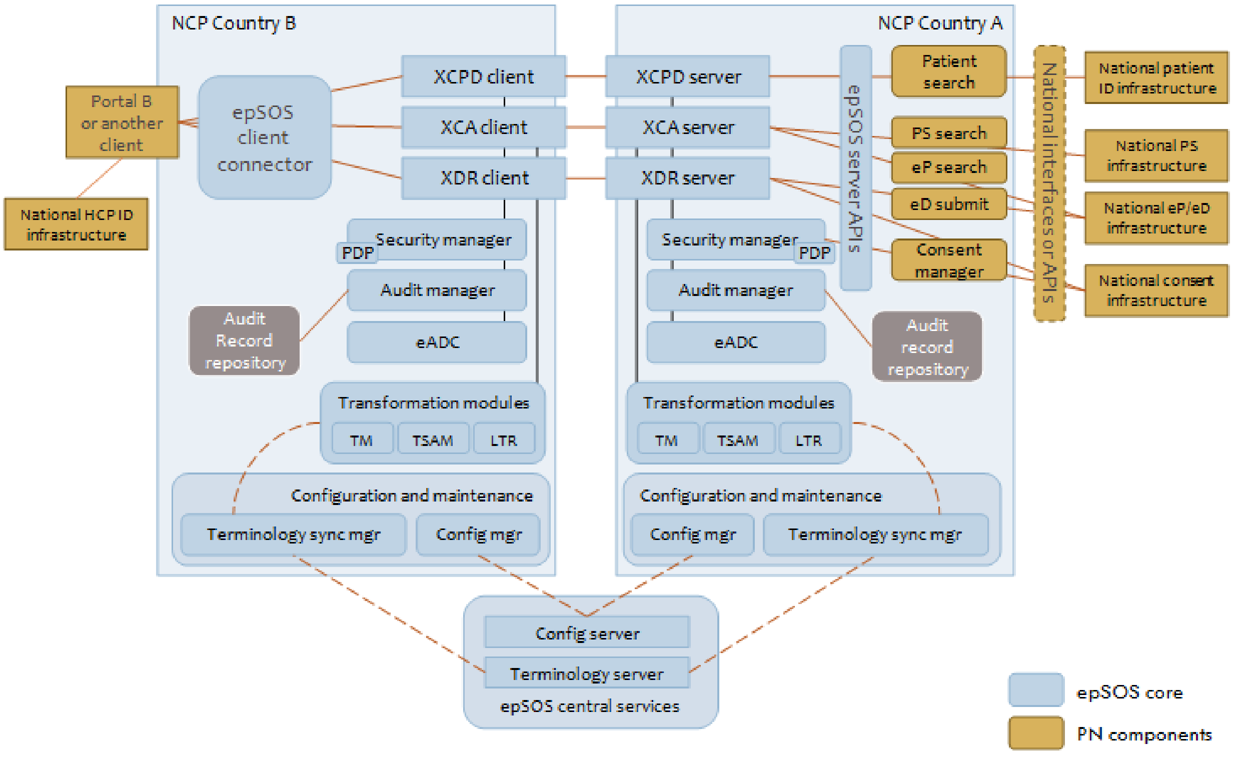


Figure 8: epSOS architecture and services

Several IHE profiles were selected to define epSOS profiles as well as the HL7 CDA standard were used to specify medical documents. The IHE profiles are:

- IHE XCA (Cross Community Access)
- IHE XCPD (Cross Community Patient Discovery)
- IHE XDR (Cross Enterprise Reliable Interchange)
- IHE XCF (Cross Community Fetch)
- IHE ATNA (Audit trace and Node Authentication)
- …

SAML assertions, certificates and encrypted network are used in order to define a reliable environment for preserving authenticity and integrity of data and the non-repudiation of actions.

Functional profiles specifying the ability of the expected systems are also used. Functional profile is a subset of the functional model. Functional profiles indicate which functions are required for a certain system such as an EHR system, mHealth Apps…

The conformity to a profile is more relevant for a system/actor than the conformity to a standard. Profiles are related to a realistic implementation of a use case.

A formal process to describe profile is generally in place. It includes the following activities (not exhaustive):

- Selection of use cases: the use cases are defined by stakeholders, users that express their needs;
- Selection of standards: the choice of the set of standards and within the standards the subset that answer the needs. This task is generally the task of the developers or implementers;
- Specification of the profiles involving suppliers and stakeholders;
- Process of specification validation including the public comments period;
- Definition of the test strategy, test plan, test criteria by a third party;
- Validation of the implementation during test sessions (it could be also part of the certification process, see section 3);
- Deployment in pilot site (optional)

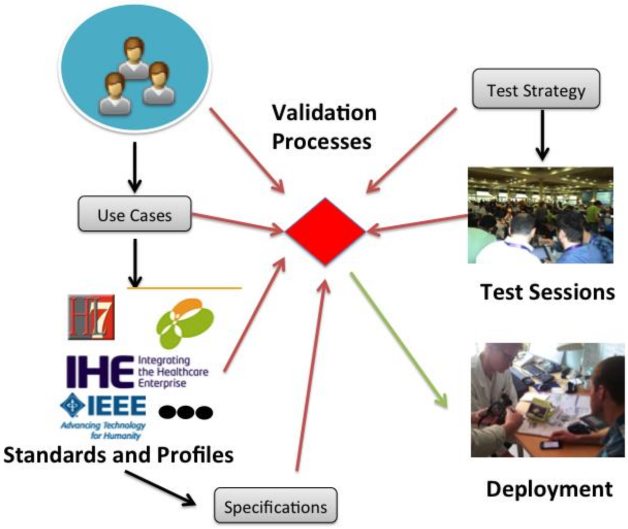


Figure 9: Life cycle and validation processes

2.4.1.2 FI-Star Guidelines and profiles

2.4.1.2.1 Methodology

An analysis of the 7 FI-STAR use cases has been done and shared with the development team of each use case:

- Bipolar Patient Treatment Management Solution (BPTM)
- Cardiac Rehabilitation (CR)
- Chronic disease Treatment Assistance Solution (CDTA)
- Diabetes Share System (DSS)
- Drug Supply Manager Solution (DSMS)
- Operating Theatre monitor Solution (TMS)
- Telecare Solution (TS)

These use cases are divided in two categories:

1. Category 1: use cases that the objectives are the monitoring of patient information using devices and mobile applications: BPTM, CR, CDTA, DSS, TS
2. Category 2: use cases that the objectives are related to the identification of objects, consumables, or medications, using barcode or RFID systems and devices (scanner, printer, antenna, etc.): DSMS, TMS. These use cases do not focus on the business workflows as the first category of use cases are doing.

We developed a questionnaire based on the solutions that are implemented. This questionnaire describes for each product/devices/systems the interoperability solutions that are implemented:

- Connectivity
- Messages and protocols

- Functions or operations that are the origin of the exchange
- Terminology and coding systems
- Security aspects

Based on the answers, we finally decided to focus our study on the category 1; the second category is more related to the identification of the objects using GTIN or GS1 identifiers.

2.4.1.2.2 The Continua Alliance defined interfaces

Continua Alliance proposes a certification process based on the requirements specified in the guidelines[19] [16].

The following schema describes the interfaces that are specified. Note that IHE and Continua has worked together to the WAN interface and Health Reporting Network (HRN) interface [13].

Continua Alliance identifies the following interfaces depending on the communication needs (see Figure 10):

- Personal Area Network (PAN) Interface for communication around a person;
- Local Area Network (LAN) Interface for communication at a location or facility;
- Wide Area Network (WAN) Interface or communication from the home/office/facility to backend services providers;
- Health Reporting Network (HRN) Interface for reporting to enterprise systems (hospitals, telehealth service providers, etc.).

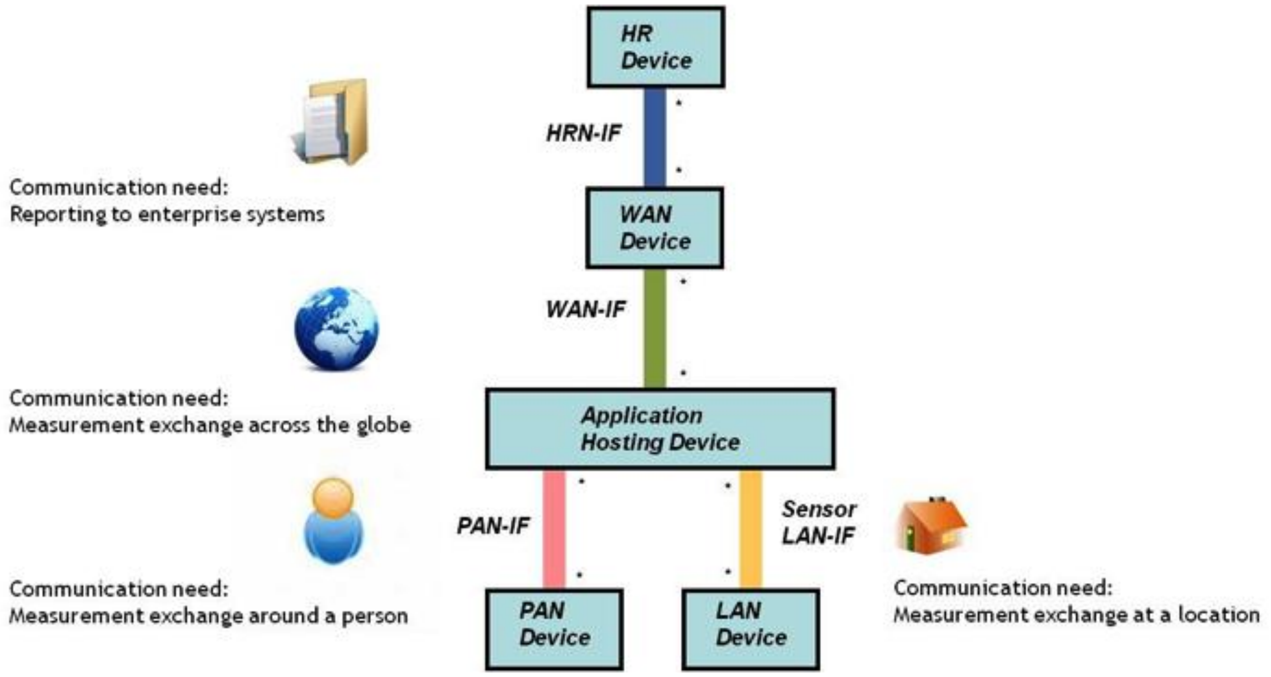

HR Device
HRN-IF
Communication need:
Reporting to enterprise systems
WAN Device
WAN-IF
Communication need:
Measurement exchange across the globe
Application Hosting Device
PAN-IF
Sensor LAN-IF
Communication need:
Measurement exchange around a person
PAN Device
LAN Device
Communication need:
Measurement exchange at a location

Figure 10: generic remote monitoring system diagram (Source Continua)

More information regarding the Continue certification process is provided in section 3.

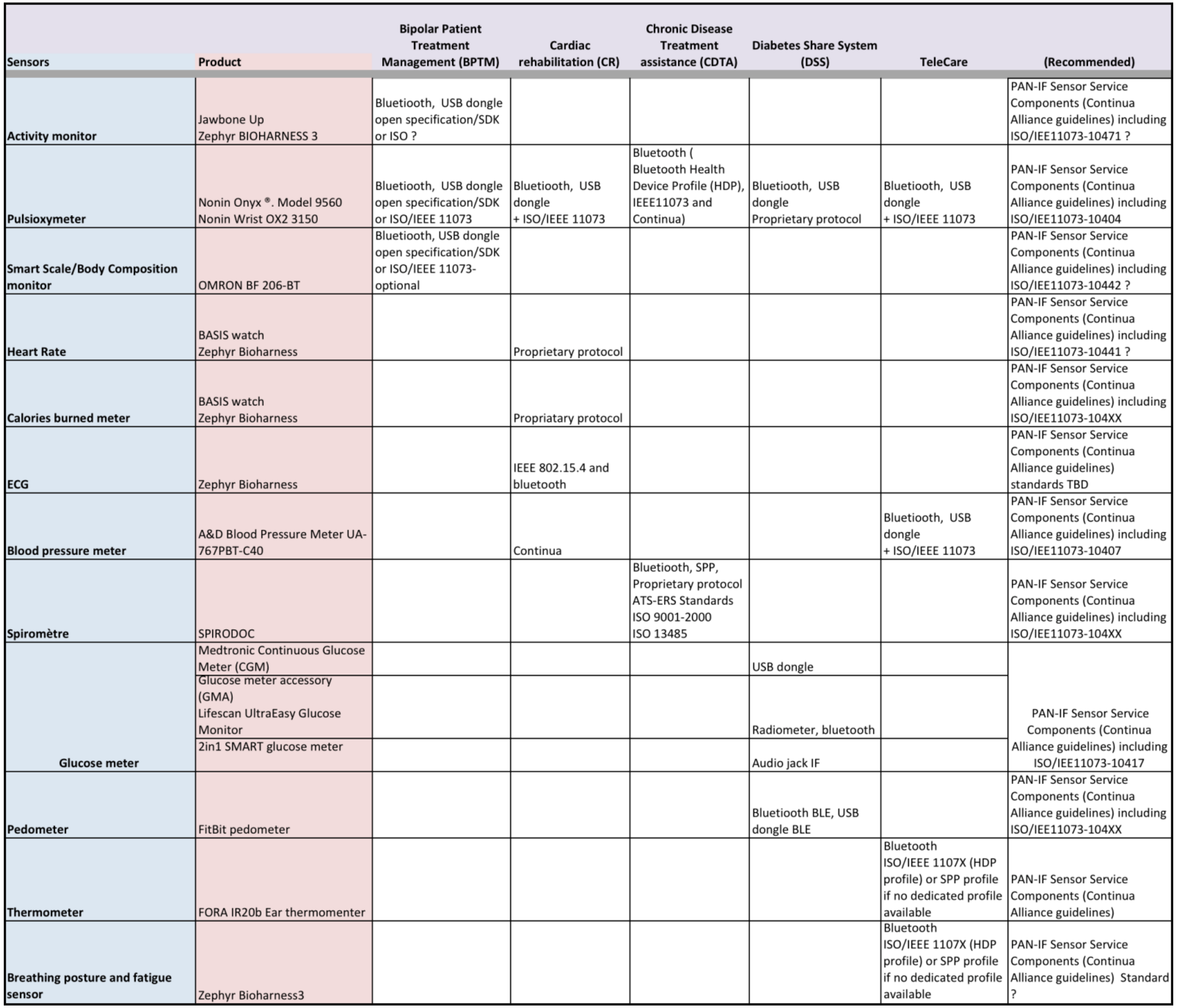
2.4.1.2.3 Category 1: using homecare devices

Analysis of the use cases demonstrates that the Continua architecture described in the Figure 10 is well adapted. In the two tables below, the list of the selection of profiles and standards are presented for the five use cases

- PAN and LAN devices (in Table 2)
- WAN device and HRN device (in Table 3)

[19] http://www.continuaalliance.org/products/certification-process

Table 2: Standards comparison among use cases using sensors

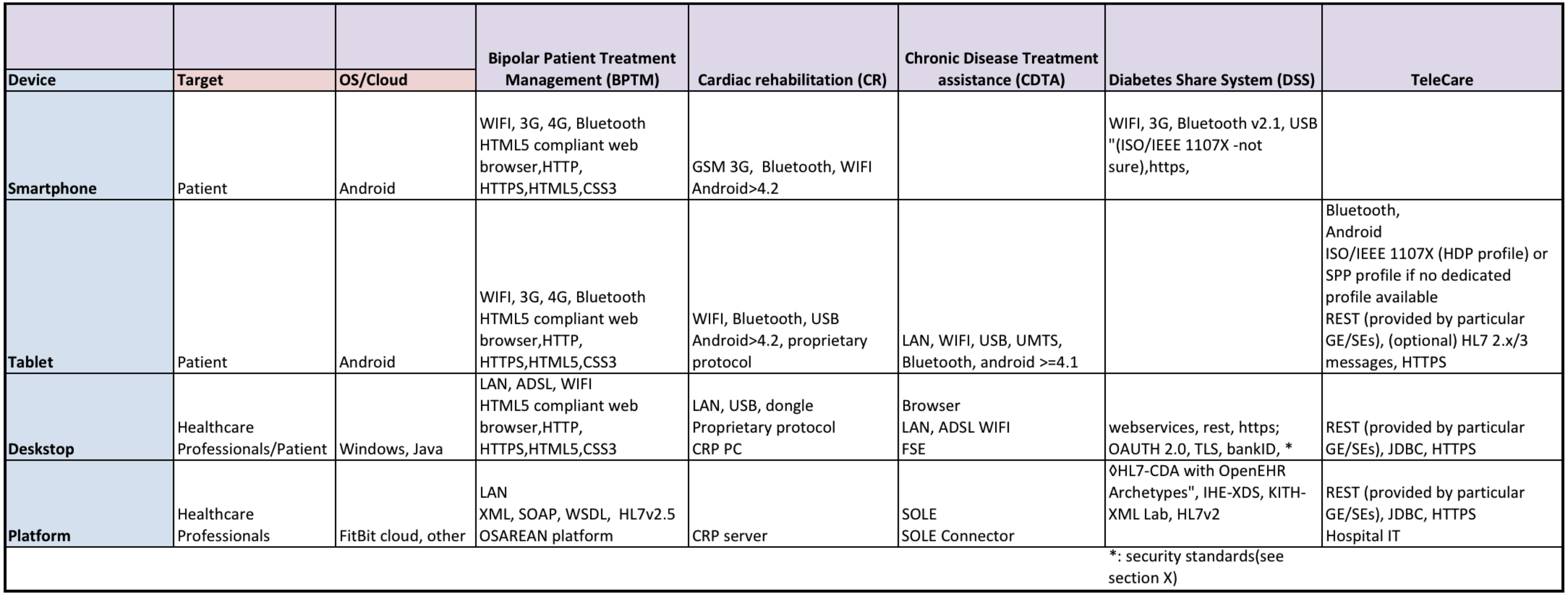


Sensors	Product	Bipolar Patient Treatment Management (BPTM)	Cardiac rehabilitation (CR)	Chronic Disease Treatment assistance (CDTA)	Diabetes Share System (DSS)	TeleCare	(Recommended)
Activity monitor	Jawbone Up Zephyr BIOHARNESS 3	Bluetiooth, USB dongle open specification/SDK or ISO ?					PAN-IF Sensor Service Components (Continua Alliance guidelines) including ISO/IEE11073-10471 ?
Pulsioxymeter	Nonin Onyx ®. Model 9560 Nonin Wrist OX2 3150	Bluetiooth, USB dongle open specification/SDK or ISO/IEEE 11073	Bluetiooth, USB dongle + ISO/IEEE 11073	Bluetooth (Bluetooth Health Device Profile (HDP), IEEE11073 and Continua)	Bluetiooth, USB dongle Proprietary protocol	Bluetiooth, USB dongle + ISO/IEEE 11073	PAN-IF Sensor Service Components (Continua Alliance guidelines) including ISO/IEE11073-10404
Smart Scale/Body Composition monitor	OMRON BF 206-BT	Bluetiooth, USB dongle open specification/SDK or ISO/IEEE 11073-optional					PAN-IF Sensor Service Components (Continua Alliance guidelines) including ISO/IEE11073-10442 ?
Heart Rate	BASIS watch Zephyr Bioharness		Proprietary protocol				PAN-IF Sensor Service Components (Continua Alliance guidelines) including ISO/IEE11073-10441 ?
Calories burned meter	BASIS watch Zephyr Bioharness		Propriatary protocol				PAN-IF Sensor Service Components (Continua Alliance guidelines) including ISO/IEE11073-104XX
ECG	Zephyr Bioharness		IEEE 802.15.4 and bluetooth				PAN-IF Sensor Service Components (Continua Alliance guidelines) standards TBD
Blood pressure meter	A&D Blood Pressure Meter UA-767PBT-C40		Continua			Bluetiooth, USB dongle + ISO/IEEE 11073	PAN-IF Sensor Service Components (Continua Alliance guidelines) including ISO/IEE11073-10407
Spiromètre	SPIRODOC			Bluetiooth, SPP, Proprietary protocol ATS-ERS Standards ISO 9001-2000 ISO 13485			PAN-IF Sensor Service Components (Continua Alliance guidelines) including ISO/IEE11073-104XX
Glucose meter	Medtronic Continuous Glucose Meter (CGM)				USB dongle		PAN-IF Sensor Service Components (Continua Alliance guidelines) including ISO/IEE11073-10417
	Glucose meter accessory (GMA) Lifescan UltraEasy Glucose Monitor				Radiometer, bluetooth		
	2in1 SMART glucose meter				Audio jack IF		
Pedometer	FitBit pedometer				Bluetiooth BLE, USB dongle BLE		PAN-IF Sensor Service Components (Continua Alliance guidelines) including ISO/IEE11073-104XX
Thermometer	FORA IR20b Ear thermomenter					Bluetooth ISO/IEEE 1107X (HDP profile) or SPP profile if no dedicated profile available	PAN-IF Sensor Service Components (Continua Alliance guidelines)
Breathing posture and fatigue sensor	Zephyr Bioharness3					Bluetooth ISO/IEEE 1107X (HDP profile) or SPP profile if no dedicated profile available	PAN-IF Sensor Service Components (Continua Alliance guidelines) Standard ?

In the last column, interoperability profiles and standards recommendations are proposed. It shows that further international specifications are needed for some of the implemented devices.

Some of the sensors are already certified Continua Alliance[20].

Table 3: standards comparison



Device	Target	OS/Cloud	Bipolar Patient Treatment Management (BPTM)	Cardiac rehabilitation (CR)	Chronic Disease Treatment assistance (CDTA)	Diabetes Share System (DSS)	TeleCare
Smartphone	Patient	Android	WIFI, 3G, 4G, Bluetooth HTML5 compliant web browser,HTTP, HTTPS,HTML5,CSS3	GSM 3G, Bluetooth, WIFI Android>4.2		WIFI, 3G, Bluetooth v2.1, USB "(ISO/IEEE 1107X -not sure),https,	
Tablet	Patient	Android	WIFI, 3G, 4G, Bluetooth HTML5 compliant web browser,HTTP, HTTPS,HTML5,CSS3	WIFI, Bluetooth, USB Android>4.2, proprietary protocol	LAN, WIFI, USB, UMTS, Bluetooth, android >=4.1		Bluetooth, Android ISO/IEEE 1107X (HDP profile) or SPP profile if no dedicated profile available REST (provided by particular GE/SEs), (optional) HL7 2.x/3 messages, HTTPS
Deskstop	Healthcare Professionals/Patient	Windows, Java	LAN, ADSL, WIFI HTML5 compliant web browser,HTTP, HTTPS,HTML5,CSS3	LAN, USB, dongle Proprietary protocol CRP PC	Browser LAN, ADSL WIFI FSE	webservices, rest, https; OAUTH 2.0, TLS, bankID, *	REST (provided by particular GE/SEs), JDBC, HTTPS
Platform	Healthcare Professionals	FitBit cloud, other	LAN XML, SOAP, WSDL, HL7v2.5 OSAREAN platform	CRP server	SOLE SOLE Connector	◊HL7-CDA with OpenEHR Archetypes", IHE-XDS, KITH-XML Lab, HL7v2	REST (provided by particular GE/SEs), JDBC, HTTPS Hospital IT
						*: security standards(see section X)	

Using the concepts of Continua Alliance guidelines, the HRN and WAN devices exchanges are today defined and are listed in the next section.

[20] see http://www.continuaalliance.org/products/product-showcase

2.4.1.2.4 FI-STAR profiles definition process

FI-STAR Use cases description shows that even if several standards and profiles are used, new profiling are needed.

An interoperability profile can be defined as a global function of exchange between two actors in a system that implements this interoperability function. For example, the IHE MHD profile defines a simple HTTP interface to an XDS environment. It defines transactions to submit a new document from the mobile application to a document receiver (actor), get or find a document based on query parameters and retrieve a copy of specific document.

A profile is composed by a set of standards from protocol communication to semantic and messages that answer to the specific needs defined in the use case. In the case of IHE-MHD, the underlying standards are

- RFC2616 IETF Hypertext Transfer Protocol – HTTP/1.1
- RFC3986 IETF Uniform Resource Identifier (URI): Generic Syntax
- RFC4627 The application/json Media Type for JavaScript Object Notation (JSON)
- RFC6585 IETF Additional HTTP Status Codes
- RFC4287 The Atom Syndication Format

The Figure 9 shows the global process of definition of profiles. The validation processes should be adapted to the context.

In the context of standard body, a strict validation process is in place and clearly described on the dedicated website. For example, the process of definition of IHE profile is available on-line at [14] and further described in the IHE wiki[21]. FI-STAR has interest to contribute to such committee for their own needs. However, FI-STAR should organise itself ahead in order to increase the efficiency of the process. The FI-STAR process would be

- Definition of the needs and the common use cases
- First selection of standards
- Write a proposal and rational
- Contribute to the international committee in charge of the domain
- Write the profile specifications
- Participate to the validation of the profile in the committee

Once the specifications are validated, FI-STAR can contribute to the development of the test tools (see section 3).

The following table presents in summary the recommended standards and profiles. All can be candidates for the quality label or certification (QL&C) requirements that FI-STAR can refer for its own purposes in WP6.

However in practical, all these standards are today implemented by the products, for example, some glucometers implement proprietary messages and have their own communication protocol (SFP on Bluetooth). The question is how to stress vendors for implementing international standards for the benefit of all.

[21] See http://wiki.ihe.net/index.php?title=Process

Personal Area Network (WAN) and local network Interface (LAN)

Data and messages

- Glucose meter: ISO/IEEE 11073-10417
- Blood Pressure: ISO/IEEE 11073-10407
- Pulse Oximeter: ISO/IEEE 11073-10404
- Automated pill dispensing systems – Medication Monitor: ISO/IEEE 11073-10471)
- Cardiovascular: ISO/IEEE 11073-10441
- Activity Hub: ISO-IEEE 11073-10471

Semantic

- IHE RTM (Rosetta Terminology Mapping)

Transport

- Optimised Data Exchange: ISO-IEEE 11073 – 20601/20601a

Communication Protocol

- USB Personal Health
- Bluetooth BT Health Device Profile (HDP)
- Zigbee Health care Profile (HCP) IEE 802.15.4

Wide Area Network Interface

Data and messages

- HL7 v2.6 constrained by IHE DEC PCD-01 and RTM
- IHE-BPPC (Basic Patient Privacy Consents)

Semantic

- IHE RTM
- IEEE 11073-20601 and 104XX terms
- IEEE 11073-10101 terms and -10201 info model

Transport

- IHE DEC PCD-01

Communication Protocol and security

- Web services WS-I Basic Profile
- IHE-ITI TF vol 2 appendix V Rev 6.0
- WS-I over SOAP 1.2 and WSI-BSP, TLS and IHE-ATNA
- IHE-CT

Health Reporting Network Interface

Data and messages

- HL7 CDA r2
- Or HL7 CDA r1
- Or IHE-MHD (Mobile Access to Document)
- IHE-BPPC (Basic Patient Privacy Consents)

Semantic

- CCD (Continuity of Care Document)
- Personal Healthcare Monitoring report (PHMR in CCD)
- SNOMED, LOINC, UCUM
- IEEE 11073- X

Transport

- IHE XDR (Cross Enterprise Document reliable Interchange)
- IHE-XDM (Cross Enterprise Document Media Interchange)
- IHE-CT

Communication Protocol and security

- Direct communication: MTOM, SOAP 1.2, HTTP(S)
- Email/media: Zip format/S-MIME or media
- Mobile: HTTP, JSON, RESTful or HL7 FHIR (in progress),
- IHE-ATNA (secure Node (X509 certificate, TLS) or Secure Application and audit messages (RFC 5424, 5425, 5426))
- IHE-IUA (Internet User Authorization) (OAuth 2.0, JWT token, SAML token)

In the case of mobile applications, IHE is planning to develop new profiles in 2013-2014 in the field of mobile application.

IHE defined a document architecture called IHE XDS. Other related profiles are also needed such as IHE-PIX, IHE-PDQ and IHE-XUA.

2.5 Summary and conclusion

Legal norms, ethical opinions and technological standards have to be considered when planning, designing and implementing medical modular architectures based on IoT elements and Generic Enablers. In principle these norms and standards do not distinguish between hardware and software technologies or IoT and the Core Platform. In most countries software products now have to comply fully with the national medical product legislation, which has not always been the case. Although regulations are complex and diverse and might be perceived as hurdle or obstacle on the way to the development of new technologies staff and patient’s rights have to be considered and health and safety must have first priority. A detailed requirements analysis is inevitable in order to assure full compliance with regulations of new technologies and to avoid unexpected costs for adjustments and adaptation at a late stage in the development process

The technical analysis and the interoperability mapping show the following findings:

- Some of the sensors are today Continua Alliance certified. It means that the tendency is to use standards and profiles well defined specifications.
- Trainings to architects and specifications team on interoperability environment and security are more and more a pre prerequisite before starting a new project
- Specifications of new standards related to sensors that are not yet covered are required
- eHealth applications shall also developed capability to implement standards and profiles from eHealth domains such as IHE profiles, HL7 CDA…
- Patient consent has to be implemented. IHE profile is available and support such need.

3 Certification

3.1 Context of Certification in FI-STAR and FI-PPP

FI-PPP community is acting like technologies-related fora, which want to promote their technologies to the market. As market-driven fora, they are business oriented ones and hope to have the broader base of market adopters as possible, beyond a critical mass necessary to ensure return of investment as well as for reducing cost in developing competitive product or services. Some usual criteria of success are to offer market-accepted specifications and expose some complex features through open interfaces. Other important successful elements of their programme are to solidify and validate such specifications and or specifications in particular when exposing features through open API. Specific tools and pragmatic events such as plugfest are organised. Clear test cases and tools are developed to assist adopters in verifying conformity to specifications (e.g. interfaces) and ensure that development investment is not wasted by non-interoperable, non-interchangeable products. At the end fora develop validation and/or label schemes detailing the mechanism to get confidence by a label and using some more or less complex imposed routes (e.g. self-certification with free tools, going to lab with more complex approaches, etc.).

Looking at FI-PPP overall programme with all newly specified GEs, open interfaces exposed, with additional GEs providers coming, sometime implementing open source instances, a lot of SMEs integrate the program and play with GEs (phase III is considering financing 1000 SMEs), we realise that none of elements of providing confidence in the FI-PPP elements are in place and the challenges are huge to provide confidence and secure investment of adopters. Therefore, it is important to support confidence building activities with the following tasks:

1. Defining market and technologies requirements for a building confidence programme
2. Develop test and tools for sub-set of key elements of the core platform
3. Develop a building confidence programme with a label scheme ensuring long term sustainability
4. Provide support and assistance including organising of FI-PPP plugfest events

3.2 What is certification?

3.2.1 How certifying? The overall concept of certification

Certifications are organised all over the world in quite all-industrial domains either for regulators or for organisation in voluntary approach. A set of worldwide standards and guidance are successfully used worldwide (e.g. ISO Guides, ISO 9000 and ISO 17000 series) in a broad range of different sectors and for many years. It is assumed that the overall approach developed in these reference standards can be harmoniously used for a particular forum although some specific guidelines might be developed as in other sectors.

3.2.2 General presentation of certification

Evaluating and certifying conformity:

Conformity is understood to denote 'the fact that a product, system, body or even a person… meets specified requirements' (definition from ISO/IEC Guide 2)

The keyword with regards to certification of conformity is '**confidence**'. The reason for this is that conformity certification procedures have been established with the main aim of creating or strengthening the confidence which business interests may have both with regard to each other and with regard to products, goods and services placed on the market.

Although this context, originally applied in "non-regulated" sectors, the growing importance and cost effectiveness of certification has helped authorities in regulated sectors (e.g. EU directives) to use the same mechanisms and in most cases the same actors to ensure conformity to standards, which also cover safety requirements and protection of consumers. Eventually, such harmonisation was also seen as facilitating free circulation of goods and the establishment of a competitive European single market.

From the original concept of certification, the existence of potential methods for evaluating and certifying conformity derives from a demand from customers (in the broad sense of the term) to be assured of the characteristics of a product, service or body. It also derives from a demand from producers themselves, either to increase the level of quality of their production or to give their customers confidence. All conformity certification procedures are therefore based on the combined interest of the various concerned parties.

As time has gone by, various procedure have been established on the basis of this demand, irrespective of whether the latter has been explicitly expressed. These procedures, which will be examined below, all tend to have a dual objective: to evaluate and control the safety or quality of the product supplied or the service provided, and to promote confidence.

The coexistence of three elements thus appears to be of fundamental importance, namely: the **existence of demand**, the existence of a **frame of reference** which can be used to assess the entity in question and, lastly the existence of **organised procedures and structures** for carrying out this assessment.

3.2.3 Where can demand for certification come from?

‘Customers’

As is only fitting, the first category of ‘customers’ concerned by the procedures for evaluating and certifying conformity is made up of the governing authorities (i.e. whether local, national or international, private or public), with the aim of being assured that (forum) regulations are complied with.

These are followed by what are conventionally known as ‘users of collective procedures’. This obscure term covers all parties which carry out their activities within an overall framework (e.g. forum members, insurance companies, public-sector purchasers, certain major distributors, etc.) most or all of whom would like not to have to carry out conformity checks themselves on the specifications they use, in the knowledge that these specifications are usually made up of documents for collective use, such as standards. The motivating reasons for this category of ‘customers’ are of course compliance with the regulations in force, but also the quality of the bodies, goods and services concerned and the simplification of relations with their partners, both upstream and downstream in the case of distributions, for example.

Finally, there are the customers who act in an individual capacity- whether it be the final consumer or another enterprise - and who are motivated by the same factors as those mentioned above. In addition, the final consumer will seek to obtain (and more so than the other parties mentioned above) certainty on matters of safety, fitness for use and also information on these characteristics, the impartiality of which is guaranteed by the involvement of a third party. The enterprise sometimes differs from the other parties mentioned above in that its demand may related to characteristics which are not covered by documents of a collective nature, e.g. standards, but to a set of specifications which is specific thereto.

‘Suppliers’

The factors which motivate suppliers, manufactures or importers often tie in with those which motivate customers, particularly when they are faced with conformity certification procedures involving a third party: the essential factor is to be assured that the regulations in force are being complied with - even in cases where a certificate is not compulsory, in order to market the product - and also to give customers confidence and simplify dealings with them.

However, there are other motivating factors of a more directly commercial nature, the main ones being as follows : to reduce the costs of procedures which are designed to guarantee conformity to the customer and minimise the number of audits and tests by utilising a single recognised procedure rather than having to prove its conformity - sometimes in a different way - to each potential purchaser; to improve the level of quality in the enterprise in part via the discipline required for certification, but also via the expertise of the specialist body involved in this area; to gain a competitive advantage on a particular market via the 'added value' which certification represents ; and, if possible, to sell a higher price.

For FI-PPP related project, we can identify some users as

- List of primary actors:
  - SMEs: Test equipment manufacturers, network component manufacturers, services/application developers.
  - Industry: Network components manufacturers, network installations providers.
- List of supporting actors:
  - Industry: Network site developers having interest in components that must be certified in terms of performance and protocol support.
- A list of stakeholders and their interests: Operators and third party service providers.

3.2.4 What frames of reference are used to carry out the assessment?

This question has two aspects to it: the nature of the frame of reference and to what it relates. As seen above, this is because the frame of reference may be a regulation, a standard, a public contract specification, a code of professional specifications, a company standard or any type of private specifications such as safety requirements imposed by the final buyer.

However, the frame of reference may also relate to different subjects: one naturally thinks of requirements which apply to a product, but in fact requirements increasingly cover characteristics relating to the production tool itself, as with the ISO 9000 series of quality assurance standards, ISO 17025 on testing, which may even be applied within the company, or even requirements governing the qualifications of personnel.

The above considerations clearly show that the development of frames of reference used in conformity certification procedures is closed linked with the needs of the economy, as is the case with standards.

3.2.5 Who carries out the assessment and how?

The declaration of conformity:

The first option - and the simplest one - is the supplier's 'declaration of conformity', which is sometimes incorrectly referred to as 'self-certification', this being a contradiction in terms. This is a procedure whereby the supplier provides a written assurance that a product, service, etc. conforms to one or more specified requirements. This declaration of conformity may be provided either directly or following various contributions by a laboratory.

In order to assist suppliers with drawing up their declarations of conformity, the standards bodies have formulated a European standard, namely ISO 17050-1; compliance with this standard should, in addition, enable greater weight to be given to declarations of conformity vis-à-vis different customers.

It should be stressed that the declaration of conformity is the most widespread type of certification of conformity in free-market economies, in keeping with the way in which such economies are organised.

Tests and checks:

The purpose of a test is to evaluate the characteristics of a particular entity, generally by considering a specific frame of reference in relation to which conformity is to be verified, though not necessarily so: a test which is designed to determine the safety of a product may be carried out on the basis of the 'recognised state of the art', i.e. in actual fact on the basis of current scientific and technical knowledge in general; a broad measure of consideration is in this case given to the judgement of the expert carrying out the test.

In addition, a test may be performed on a particular example, without necessarily having to take into consideration series production or the repetition of actions or services (otherwise, the test becomes an integral part of a certification process). The test is carried out either by the entity in question or by an independent testing laboratory, which then issues a 'test report'.

The prime function of a check, on the other hand, is to verify that an entity conforms to a frame of reference; this is generally achieved by using the results of tests, though it may also involve other aspects, such as on-site inspections. The term ‘audits’ is used when a company’s quality assurance system is checked.

Certification procedures:

The aim of these procedures is to ascertain the conformity of an entity with respect to the chosen frame of reference. Although ‘certification’, in the widely accepted sense of the term, encompasses any procedure carried out by a party from outside the company and could thus cover certification by a ‘second party’, i.e. by the customers, it is preferable to restrict use of the term to procedures carried out by an independent body which comes from outside the entity in question and which is specifically designed to carry out such activities (third-party certification).

Certification may relate to a product (certification of products), the quality assurance system of an establishment or enterprise (quality-control system certification), the skills of an individual (personnel certification), or to a service (service certification). This is a procedure, which generally involves long-term monitoring of the certified entity to ensure that the conditions under which certification was awarded still apply.

Certification always results in a written document (certificate) issued by the certifying body by which the latter provides an assurance that the entity in question conforms to the specified requirements. Generally speaking, third-party certification of a products or services also results in the certified entity being entitled to use a mark granted to it or being authorised to use a distinctive sign.

3.2.6 Approval and accreditation

The question then arises as to what sort of credibility should be given to the various bodies which carry out the tests, audits, checks and certification referred to above and what sort of credibility should be given to the documents which they issue. In other words, who supervises the supervisors?

In this context, a distinction should be made between voluntary certification activities and activities which arise from a legal obligation, generally impinging on safety. In the latter case, the State calls on the service of a body which it both authorises and compels to carry out checks. Only bodies appointed by the State may then become involved in this area.

With regard to activities which take place in a private context (the vast majority of cases), the approach adopted varies depending on the country.

In certain cases, there is no specific framework for monitoring the activities of these bodies. Increasingly, however, procedures have been established in order to inspire confidence in their satisfactory operation, from the point of view of not only technical or organisational aspects but also ethics. The procedures concerned may be ones in which full responsibility rests on the regulatory authorities: the latter establish a legislative or regulatory framework defining the conditions under which these activities may be carried out, and checks that this has been implemented by issuing "approvals" to bodies which fulfil the required conditions. This is the case in France, for example, where product certification is regulated by a law dating from 1978 which requires, inter alia, the approval of the various certifying bodies.

Another option exists, however, which is being used increasingly: the option of accreditation, which is a procedure whereby a body representing all the business interests concerned, and which is thus endowed with authority, formally recognises that a body or individual is competent to carry out specific tasks in the various areas in question (test, audit, certification, etc.). Accreditation could thus be likened to "service certification", which is based on codes of good practice or frames of reference which are standardized internationally and which, to a large extent, originally resulted from the work of the ILAC (International Laboratories Accreditation Conference) and CASCO, the ISO Council Committee responsible for matters of conformity assessment and certification.

Virtually all the basic texts are now included in the ISO 17000 series and they lay down general criteria for:

- the operation of testing laboratories (ISO 17025)
- the assessment of testing laboratories (ISO 17011)
- test laboratory accreditation bodies (ISO guide 58)
- certification bodies operating product certification (ISO guide 65)
- certification bodies operating quality system certification (ISO guide 62, 66)
- certification bodies operating certification of personnel (ISO 17021)
- inspection bodies (ISO 17020)

It is to be noted that only testing laboratories are covered by standards for the three possible levels (operation of laboratories, evaluation of laboratories, criteria for accreditation bodies). The same work still has to be done, therefore, for the other activities.

It should be pointed out that a standard exists (ISO 10011) governing quality audits.

The accreditation bodies which now exists in several countries generally take the form of non-profit associations (COFRAC, UKAS, BELCERT, DAR, …), with their administrative boards comprising not only representatives of the public authorities but also representatives of the organisations concerned and reference expert from the sector.

To conclude this section, the extraordinary development of all these activities over the last two decades should be noted, a development which is due to a number of factors firstly, the growth of international competition has sparked “a dash for quality and safety”, thus leading to increased demand for forms of certification which are intended to demonstrate the safety and quality of products and services. In many cases, the sophistication of the technologies involved also prevents purchasers to from personally verifying the characteristics of the products they wish to buy, prompting them to call on the services of a specialist third party. Finally there is a trend towards deregulation in most economies which is leading to greater reliance on “private” voluntary procedures rather than on State control of markets.

The diagram below attempts to show the way in which the conformity certification systems are organised.

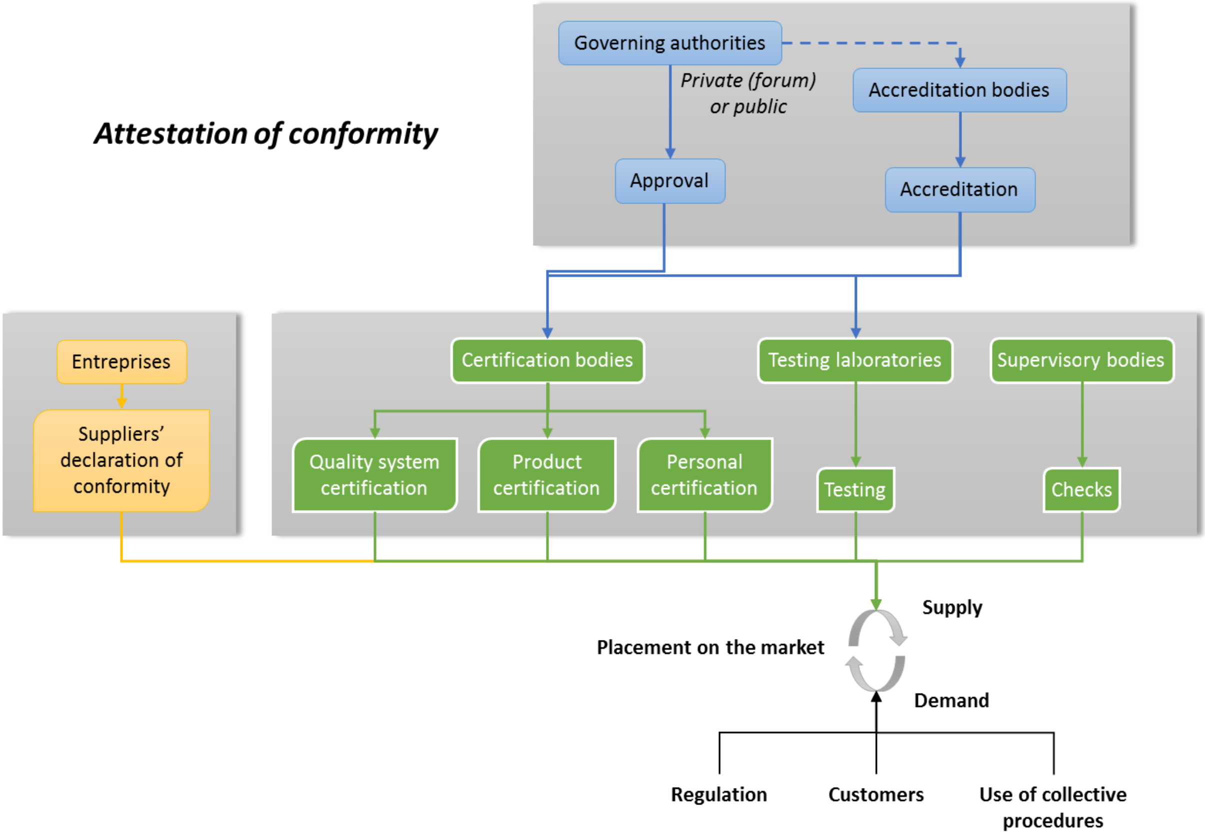


Figure 11: Overall stakeholders’ relationships in conformity assessment as to be involved in regulatory (EC Directives) or Voluntary sectors

3.3 Certification schemes

In its role of regulator and in the challenges faced by some fora in the development of the necessary instruments to create a global market, the experience in such domain of the EU regulators in front of some equivalent issues to create the European single market in all industrial sectors are worth to be outlined.

To consider "certification", it was then felt useful to bring to the attention of the reader how this aspect was dealt with within the EU for many sectors. Many issues were raised and some mechanisms developed which are worth to be considering within this report.

In its duty to organise the certification, here called "conformity assessment", EU has defined 8 conformity assessment modules and corresponding routes and schemes to combine the modules together. Choice of the modules depends on the level of security related to the fields.

Examples:

- Simplest module (e.g. module A) and route is supplier's declaration
- Intermediate module (e.g. B+C) is used in telecom fields with test in laboratory and control of production
- More complex route is with module H for instance for medical devices for full quality assurance control even of production

Here is below simplified explanation of various approach for conformity assessment where we can use concepts for FI-STAR and the whole FI-PPP programme.

3.3.1 The Council resolutions on a "new approach" and a "global approach"

The creation of a Single Market by 31 December 1992 could not have been achieved without a new regulatory technique that set down only the general essential requirements, reduced the control of public authorities prior to a product being placed on the market, and integrated quality assurance and other modern conformity assessment techniques. Moreover, the decision-making procedure needed to be adapted in order to facilitate the adoption of technical harmonisation directives by a qualified majority in the Council.

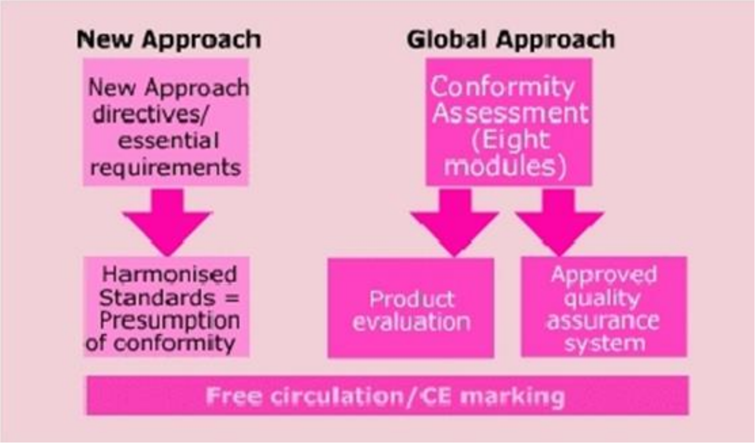

New Approach
Global Approach
New Approach directives/ essential requirements
Conformity Assessment (Eight modules)
Harmonised Standards = Presumption of conformity
Product evaluation
Approved quality assurance system
Free circulation/CE marking

Figure 12: overview of new and global approach to conformity assessment (source EOTC)

A new regulatory technique and strategy was laid down by the Council Resolution of 1985 on the New Approach to technical harmonisation and standard-isation, which established the following principles:

- Legislative harmonisation is limited to essential requirements that products placed on the Community market must meet, if they are to benefit from free movement within the Community.
- The technical specifications of products meeting the essential requirements set out in the directives are laid down in harmonised standards.
- Application of harmonised or other standards remains voluntary, and the manufacturer may always apply other technical specifications to meet the requirements.

- Products manufactured in compliance with harmonised standards benefit from a presumption of conformity with the corresponding essential requirements.

In addition to the principles of the New Approach, conditions for reliable conformity assessment are necessary. The key elements in this respect are the building of confidence through competence and transparency, and the setting up of a comprehensive policy and framework for conformity assessment. The Council Resolution of 1989 on the **Global Approach to certification and testing** states the following guiding principles for Community policy on conformity assessment

The New Approach entailed refining conformity assessment in such a way as to allow the Community legislator to evaluate the consequences of the utilisation of different conformity assessment mechanisms. The objective was to provide flexibility of conformity assessment over the entire manufacturing process in order for it to be adapted to the needs of each individual operation. The Global Approach introduced a modular approach, which subdivided conformity assessment into a number of operations (modules). These modules differ according to the stage of development of the product (for example design, prototype, full production), the type of assessment involved (for example documentary checks, type approval, quality assurance), and the person carrying out the assessment (the manufacturer or a third party).

The Global Approach was completed by Council Decision 90/683/EEC, which was replaced and brought up to date by Decision 93/465/EEC. These decisions lay down general guidelines and detailed procedures for conformity assessment that are to be used in New Approach directives. Thus, conformity assessment is based on:

- manufacturer’s internal design and production control activities
- third party type examination combined with manufacturer’s internal production control activities
- third party type or design examination combined with third party approval of product or production quality assurance systems, or third party product verification
- third party unit verification of design and production, or
- third party approval of full quality assurance systems

In addition to laying down guidelines for the use of conformity assessment procedures in technical harmonisation directives, Decision 93/465/EEC harmonises the rules for the affixing and use of the CE marking. The subdivision of a conformity assessment procedure into modules is either based on the intervention of a first party (manufacturer) or a third party (notified body), and relates to the design phase of products and/or to their production phase. Should manufacturers subcontract either design or production, they still remain responsible for the execution of the conformity assessment procedures for both phases. The modules are quickly described here below in Figure 13 and Figure 14.

3.3.2 The 8 modules of conformity assessment (A to H)

The modules give the legislator, in relation to the type of products and risks involved, the means to set up the appropriate procedures for manufacturers in order to demonstrate product conformity against the provisions of the directive.

As a result of the modular approach, the New Approach directives establish different procedures, according to the categories of products covered, by either leaving manufacturers no choice within the same category, or by giving them the freedom of choice within the same category of products. Alternatively, the directives can also establish, for all the products covered by the scope, a range of procedures from which the manufacturer must choose. Table 4 shows a summary of the modules provided for in each New Approach directive. Detailed flowcharts of the conformity assessment procedures according to each New Approach directive can be found in the directive.

Providing a choice under a New Approach directive between two or more conformity assessment procedures for the same product may be justified, where different certification infrastructures have developed in the Member States as a result of different legislation. Still, the Member States must transpose into their national legislation all the conformity assessment procedures established under a directive and they must guarantee the free movement of all products, which have been subject to a conformity assessment procedure applicable to the directive in question. The choice of modules may also be justified, where a product is subject to the provisions of more than one directive. In these cases the manufacturer should be able to apply a common procedure contained in all the relevant directives or at least procedures which are compatible. Finally, a choice may also be justified on the basis of the infrastructure of the branch of industry concerned to enable manufacturers to choose the most suitable and economic procedure.

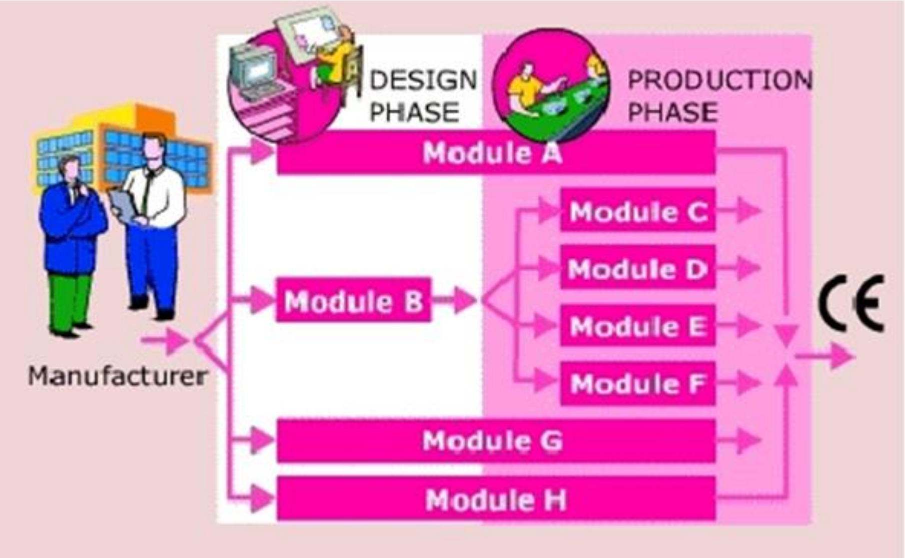
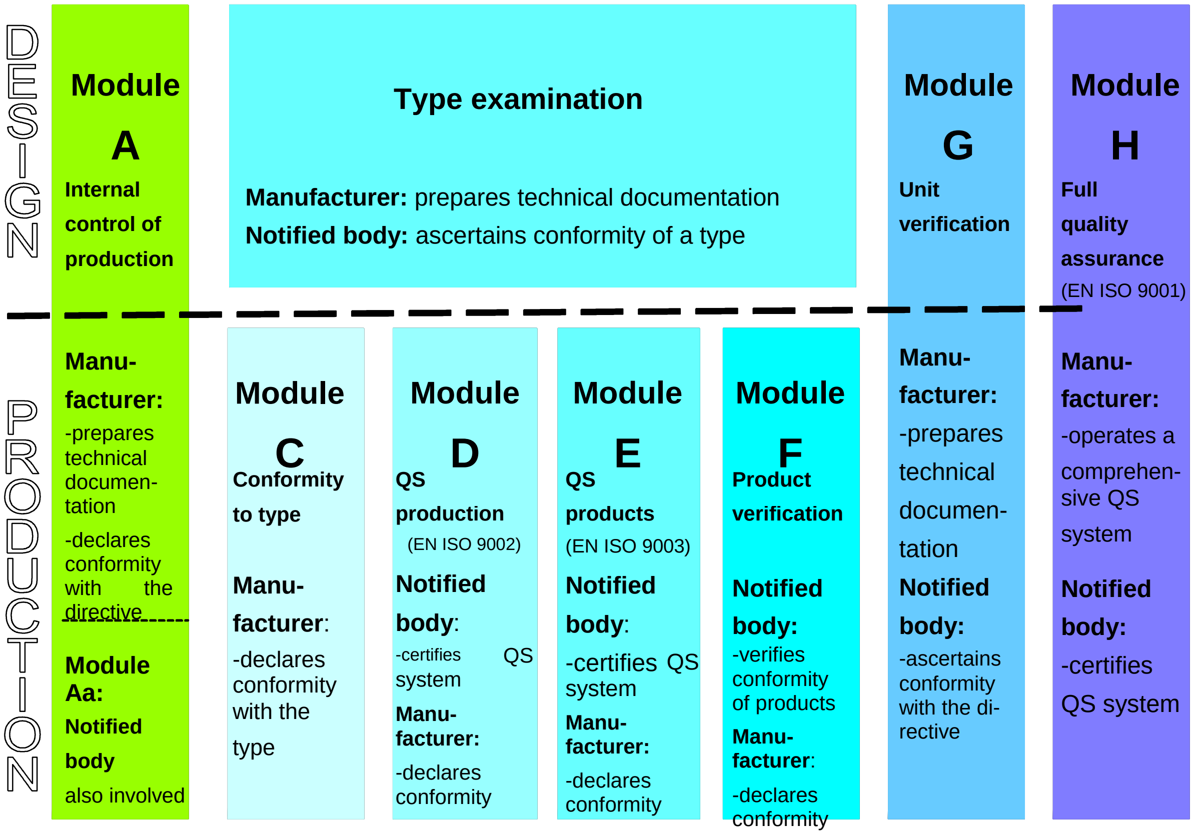


Figure 13: the 8 modules of conformity assessment (source EOTC)



Module A
Internal control of production

Type examination

Manufacturer: prepares technical documentation
Notified body: ascertains conformity of a type

Module G
Unit verification

Module H
Full quality assurance
(EN ISO 9001)

Manufacturer:
-prepares technical documentation
-declares conformity with the directive

Module Aa:
Notified body also involved

Module C
Conformity to type
Manufacturer:
-declares conformity with the type

Module D
QS production
(EN ISO 9002)
Notified body:
-certifies QS system
Manufacturer:
-declares conformity

Module E
QS products
(EN ISO 9003)
Notified body:
-certifies QS system
Manufacturer:
-declares conformity

Module F
Product verification
Notified body:
-verifies conformity of products
Manufacturer:
-declares conformity

Manufacturer:
-prepares technical documentation
Notified body:
-ascertains conformity with the directive

Manufacturer:
-operates a comprehensive QS system
Notified body:
-certifies QS system

Figure 14: Modules as defined in COUNCIL RESOLUTION of 21 December 1989 on a global approach to conformity assessment (90/C 10/01).

By including in the New Approach directives modules based on quality assurance techniques derived from the EN ISO 9000 series of standards, a link has been established between the regulated and non-regulated sectors. This should help the manufacturers to meet simultaneously the obligations based on directives and client needs. Furthermore, it allows manufacturers to benefit more from their investment in quality systems. It contributes also to the development of the quality chain (from the quality of products to the quality of companies themselves), and promotes awareness of the importance of quality management strategies for improving the competitiveness.

3.3.3 Modules provided for in New Approach directives

Table 4: Summary of the modules provided for in each New Approach directive

	DESIGN + PRODUCTION MODULES							PRODUCTION MODULES		
Directives	A	B+C	B+D	B+E	B+F	G	H	D*	E*	F*
87/404/EEC Simple pressure vessels		x(+)			x					
88/378/EEC Toys	x	x								
89/106/EEC Construction products	x		x					x		
89/336/EEC Electromagnetic compatib.	x x (+)	x								
89/392/EEC Machinery	x	x								
89/686/EEC Personal protective equip.	x	x x (+)	x							
90/384/EEC Non automatic weighing instruments			x		x	x		x		x
90/385/EEC ***Active implantable medical devices***			x		x		x (+)			
90/396/EEC Gas appliances		x (+)	x	x	x	x				
91/263/EEC ***Telecommunications terminal equipment***	x	x (+)	x				x			
92/42/EEC Hot-water boilers		x (+)	x	x						
93/15/EEC Explosives for civil uses		x (+)	x	x	x	x				
93/42/EEC ***Medical devices***	x (+)		x	x	x		x (+)	x	x	x
94/9/EC ATEX	X	x	x	x	x	x				
94/25/EC Recreational craft	x x (+)	x	x		x	x	x			
95/16/EC Lifts		x(+)	x	x	x	x	X x(+)			
96/57/EC Energy efficiency for refrigerators and freezers	X									
97/23/EC Pressure equipment	x x (+)	x(+)	x B1 + D	x	x B1 + F	x	x x (+)	x	x	
73/23/EEC LVD	X									

Legend:

* = additional requirement for a technical file

(+) = with supplementary requirements

B1= a special module that cannot be found in the other directives

3.4 Some certification programmes

3.4.1 Case of regulated certification: CE mark

The CE marking (also known as CE mark) is a mandatory conformance mark on many products placed on the European ‘single market’. The CE marking certifies that a product has met EU consumer safety, health or environmental requirements. CE stands for Conformité Européenne, (European conformity) in French.

The CE marking is a mandatory marking for certain product groups to indicate conformity with the essential requirements set out in European Directives – especially safety-related directives, such as the Medical Device Directive (Council Directive 93/42/EEC of 14 June 1993 concerning medical devices, revised in 2007), Low Voltage Directive and the Machinery Directive.

Under the New Approach the Medical Device sets out safety goals as “essential requirements” rather than saying how to achieve them. It is through international standards that manufacturers learn how to develop and assess their products. Standards useful for assuring essential requirements are called “harmonized standards” and a list of harmonized standards is published in the Official Journal of the EC. For safety aspects in Medical Devices, the standards family IEC 60601 has been harmonized, with clause 14 in 60601-1 mentioning software in Medical Devices. IEC 62304 describes process measures for software in medical devices. **Note that the revised Medical Device Directive includes software that itself can be seen as a medical device, but there is no standard describing the software product being a medical device in its own right – though standard bodies are willing to close this gap soon (see §3.6.3).**

3.4.2 Introduction to ehealth certification

In e-Health sector relatively young on the deployment of wide and large system where thousands of patients and several types of health organisations are involved, standards are the key for the success of such projects. epSOS project [9] by using IHE profiles and underlying standards have been a major demonstration of the use of existing standards to define national contact point for exchanging medical data across Europe. **A testing platform, test criteria, testing tools and validation process was the first step for a quality assurance process**.

In United States, meaningful use has the goal of promoting the spread of electronic health record to improve health care. The ONC (Office of the National Coordinator for Health IT) identifies standards and certification criteria.

In Europe, several countries develop national certification on EHR: Belgium, Ireland, France, Slovenia, … but in term of interoperability, **the main reference of quality label is the IHE Connectathon platform** where companies test against their pairs conformance and interoperability workflows that are defined in the IHE technical frameworks developed in different domains such as radiology laboratory, infrastructure, Patient care Devices and many others. A quality label is today well defined and subject to ISO 17025 audit. It means that IHE-Europe and its services regrouping in IHE-services will be able to become an ISO17025 Conformance Assessment Body (CAB). Continua Alliance with the Continua guidelines that provide a general overview of interoperability architecture for the homecare devices, describes a certification process[22].

The European Commission with DG Connect delivered recently the eHealth Interoperability Framework[23]. These deliverables were developed in 2012 with the support of the experts, industry and stakeholders of the eHealth domain and are used today as an input of the Antilope project that the aim is to support adoption and take up of standards and profiles for eHealth. The project will provide guidelines, recommendations and frameworks based on a set of use cases, related profiles and standards, Interoperability Quality Management System, testing guidelines and Certification process. The scalability of the results to the EIP on Active and Healthy Ageing is also considered.

[22] www.continuaalliance.org

[23] http://www.ehealthnews.eu/download/publications/3474-ehealth-interoperability-framework-study

All the deliverables will be presented for validation and promotion by organizing ten workshops across Europe covering a region of countries based on proximity.

The eHealth European Interoperability Framework [9] proposes 10 use cases where two are directly issued from the epSOS project, four use cases that suit to a deployment of a national/regional HIE (Health Information Exchange), two are dedicated to hospitals and the two last use cases focusing on homecare. These use cases are all supported by IHE profiles (Cross sharing or exchanging document, security environment, patient and healthcare identifications, laboratory or radiology workflow) and the Continua Alliance guidelines for the homecare use cases. Semantic is also included within the profiles. Today a refined eEIF is on preparation in Antilope project [17]. This framework lists 8 use cases but for some of them a clear distinction is made to distinguish the scalability of the use case, cross border, national/regional or local levels.

For the deployment of the certification process based on such profiles, IHE (Integrating the Health enterprise) has been developing for up to ten years test tools and test platform conformed to the GITB recommendations [21]. This generic platform can be adapted for other development on eHealth interoperability use cases.

Concerning functional requirements derived from European and international standards, EuRorec[24] has also developed a platform and tools offering a large set of functional statements. By selection of a set of requirements corresponding to the products or systems that will be deployed (called also functional profiles), an organization or country can easily defined its functional certification program coupled with the interoperability certification.

Antilope project finally describes the functional roles of entities that participate to the QL & Certification processes in eHealth mixing European and national/regional levels in order to harmonise the different levels of assessments by using common standards and profiles in the project and allowing extensions for the specific needs of the project.

QL& certification processes are today endorsed by consortium such as Continua Alliance, IHE-Europe, for the functional aspects by EuroRec and for medical devices the CE mark. The processes are generic but very often, regulation in countries promote national/regional certification for specific purposes (ePrescription, transmission of data for reimbursement, national EHR systems,).

3.4.2.1 Case of private certification: Continua Alliance

Continua Alliance issues a certificate. It gives to the product a recognizible Continua Certified™ logo. The certification has two objectives: conformance testing against the Continua Alliance specifications and interoperability testing (PAN devices only). The devices having passed the certification are published at the Continua website[25]. The testing tools used by Continua Alliance and responding to the eEIF and its use cases are described in the Antilope Workpackage 3 (in progress in October 2013)

3.4.2.2 IHE (Integrating the Healthcare Enterprise)

IHE has been developing interoperability profiles in different eHealth domains since more than ten years: Anatomic Pathology, Cardiology, Eye care, IT Infrastructure, Laboratory, Patient Care Coordination, Patient Care Devices, Pharmacy, Quality, Research and Public Health, Radiation Oncology, and Radiology. IHE-Europe collaborates to the Continua Alliance guidelines where some of the existing IHE profiles are included. IHE is developing new profiles in the Mobile Health applications.

IHE develops extensively test methods and test tools and continuously upgrades and automates its testing methods and tools in the project called Gazelle. The Gazelle test bed[26] is compliant with the GITB specifications [13].

[24] http://www.eurorec.org

[25] http://www.continuaalliance.org/products/product-showcase

[26] http://www.ebusiness-testbed.eu

Every year, IHE organises testing sessions called Connectathon over the world: North America, Europe, Japan, Australia, Korea, etc. The passed companies for specific profiles are published at http://www.ebusiness-testbed.eu.

IHE does not provide any QL or certificate to the products. The process can be considered as a quality process. IHE organises Projectathon for specific projects such as epSOS project. IHE defines the testing strategy, test methods, develops extensions or new test tools, organises testing sessions (virtual or face to face testing sessions for the project.

The testing tools are available on line at http://gazelle.ihe.net.

IHE-Europe is developing interoperability testing services with high level of quality. All the team is today ISTQB qualified.

3.5 Standardization and certification in data protection law

Currently, the EU Data Protection Directive ('DPD') [29] does not contain mandatory requirements of standardization or certification of IT products or IT-based services. The use of data protection standardization and certification schemes in Europe is mostly a voluntary, self-regulatory measure. Most references in law to the data protection and security standards are quite general. Few legal rules contain a stronger link to particular standards.

3.5.1 Data protection certification schemes

Currently, different groups of organizations can establish certification schemes (e.g. trust marks or seals of approval) based on self-imposed voluntary standards by means of codes of conduct, to certify that a provider/producer of an IT service/product complies with the requirements of the code. Such certification schemes are administered by the code of conduct 'owners' [30].

Article 27(1) DPD encourages the drawing up of industry codes of conduct to properly implement the data protection standards of the DPD in the specific context individual industries and sectors. The examples of sectors where such codes of conduct exist are the financial services[27] and the public transportation sectors[28]. The DPD does not require a formal approval of such codes by public authorities. The codes can be adopted both at the national and European level and can be – if the code 'owners' so choose - approved by the national data protection authorities ('DPAs') and Article 29 Working Group – a European advisory body on the matters of data protection established by the DPD – respectively [31].

Whether or not compliance with the rules in the codes – and hence, standards of a certain certification scheme – can be enforced against participating organizations in courts depends on whether or not such codes have binding legal status. In some national legal systems, an approval of a DPA may have a determining effect: e.g., while in the Netherlands, such approval is not binding for courts, whereas in Ireland approved codes become legally binding.

Data protection certification can be administered either by an independent private entity, or – as it has been done in some EU member states – by national DPAs. The privately-administered data protection (privacy) seals mostly originate in the US: Trust Guard, TRUST-e, BBB, etc. Their effectiveness and reliability have been criticized because of a controversial position private administrators of the seals occupy: they have to balance their mission to ensure a compliant level of data processing and generate revenue from participating companies [32]. In some member states, public authorities - national DPAs - take over the role of a seal administrator and issue data protection seals certifying compliance with local data protection law. The data protection authority of the German Land of Schleswig-Holstein (the 'ULD') [33] issues such a seal. The law of Schleswig-Holstein prescribes for the public bodies of that State, when procuring IT-based

[27] E.g. De gedragscode voor de verwerking van persoonsgegevens van de Nederlandse Vereniging van Banken en het Verbond van Verzekeraars (the Code of conduct of the Dutch Bank Association and the Union of the Insurance companies regarding the processing of personal data) approved by the Dutch DPA on the 13th of April, 2010

[28] E.g. Gedragscode verwerking persoonsgegevens OV-chipkaart door OV-bedrijven (The Code of conduct regarding processing by the public transport companies of personal data in relation to the public transport chip card) the most recent available version of which was registered by the Court of the Hague on the 13th of February 2009, no. 16/2009

products and services, to give preference to the ones that have been certified [34]. The French DPA (CNIL) issues a similar data protection label [35].

Other examples of existing certification schemes include Portugal's PACE issued by the Portuguese E-commerce Association (privately managed seal), and the Danish e-mark administered by the e-commerce Foundation (privately managed seal) [36].

3.5.2 Privacy Seals and Privacy Certification

Privacy seals certify the compliance (compatibility) of ICT products and services with European (e.g. 95/46/EC and 2002/58/EC) and/or national privacy/ data protection and data security laws after the completion of a specific documented procedure performed by accredited legal and technical experts and after approval of the evaluation by the experts by the certifying organization.

Opinion 3/2010 of the Article 29 Working Party (WP173) [52] points out that the accountability principle could impact the development of certification programs or seals, as data controllers may decide to use the option of trustworthy services delivering certificates. It is expected that data controllers will favour seals known for their rigorous testing as these certificates will provide more 'compliance comfort' in addition to offering competitive advantage. The seal issued to the controller of personal data would confirm the privacy assurances given by the data controller and this could assist the data protection authority in assessing whether the data controller provides sufficient safeguards for the purposes of (international) data transfers.

Certification of privacy seals and other privacy certification schemes is currently high in the European agenda and the European Joint Research Centre has commissioned a study on European privacy seals, the results of which have not yet been made public [52].

3.5.2.1 EuroPriSe (European Privacy Seal) [52]

On a European level, there is a EuroPriSe (European Privacy Seal), a voluntary data protection certification scheme for IT products and IT-based services that comply with the EU data protection laws, taking into account the national legislation of the Member States [52].

The scheme has been developed as a result of an EU-funded research project (involving a consortium of nine partners from eight EU Members States with different legal and certification cultures conceptualised EuroPriSe in the frame of the EU eTEN programme (project no.046221)). The resulting seal has been highly rated on the criterion "supportive on EU policies on data protection, compliance and application and directly relevant to EU policies in trust and security" [52].

Currently, the Independent Centre for Privacy Protection Schleswig-Holstein (ULD), the German Data Protection Authority of the State of Schleswig-Holstein operated the EuroPriSe. As of 01 January 2014 the operations will be transferred to a new entity, EuroPriSe GmbH.

The **EuroPriSe standards** – as provided for in the EuroPriSe catalogue [52] - draw on the DPD, Directive on Privacy and Electronic communications 2002/58/EC, court rulings, and Article 29 Working Party opinions, also accounting for the national implementation. The EuroPriSe criteria are presented in a number of practical questions are technology-neutral and flexible [52].

The certification process involves evaluation of an IT product or service by a third party expert on the matter of compliance with the EuroPriSe criteria, and a validation by an impartial certification authority. The evaluation of an **IT product** involves assessment of the documentation, standard configurations, and laboratory testing of the product. The evaluation of an **IT-based service** involves assessment of the service implementation, and may involve situ audit [52].

The evaluation is conducted by **external experts** who are trained and tested by the EuroPriSe. The seal is issued by **EuroPriSe Certification Bodies**, impartial and independent authorities with expertise in privacy and data protection.

3.5.3 Standardisation and certification in the area of data security

3.5.3.1 Requirements for secure electronic signatures

Security of electronic signatures is one area of law, which refers to standards and (voluntary) certification. Several FI-STAR use cases may use electronic signatures as a means of authentication to ensure that access to personal data processed is only granted to authorized persons.

Directive 1999/93/EC [52] (the ‘eSignature Directive’) establishes the criteria for legal recognition of electronic signatures via certification services that could be provided both by private bodies and public authorities in the EU member states.

It defines ‘electronic signature’ as ‘data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication’ (Article 2(1)).

The Directive establishes:

- common obligations for certification service providers;
- common rules on liability;
- cooperative mechanisms to facilitate trans-border recognition of signatures and certificates with third countries

Annex I of the Directive contains requirements for qualified certificates; Annex II contains Requirements for certification-service-providers issuing qualified certificates, and Annex III establishes the requirements for secure signature-creation devices respectively.

The European Commission adopted a decision on the publication of reference numbers of generally recognised standards for electronic signature products [52]. This Decision refers to three generally recognized standards for electronic signature products which presume compliance with the qualified electronic signature.

3.5.3.2 Security requirements for mobile apps

Many public and private parties (operation system- and device manufacturers) have published guidelines regarding security in general and security of mobile apps in particular [52]. The Article 29 Working Party made recommendations for security measures relevant for multi-layered platforms, such as the ones developed by the FI-STAR project, in its Opinion 02/2013 on apps on smart devices adopted on 27 February 2013. For a detailed overview of those requirements we refer to D1.1.

3.5.3.3 Security requirements related to mandatory data security breach notifications

FI-STAR deliverable D1.1 has already discussed legal requirements related to data security breach notifications. This section focuses on the technological measures that are exempt from an obligation to notify a subscriber or individual concerned about the data breach (national competent authorities have to be notified in any circumstances).

To restate the EU law on data security breach notification, currently, only the so-called ePrivacy Directive [52] imposes, in article 4, an obligation on providers of publicly available electronic communications services to proactively inform users of their services and national authorities. However, mandatory data security breach notification is likely to be introduced more widely in the near future as part of the review of the Data Protection Directive. Some European countries, including Austria, Germany and Norway, have already introduced general mandatory data breach notification in their national law [52], and other countries are discussing such regulations.

3.5.3.3.1 Exemption from the notification obligation

Under the ePrivacy Directive, an entity under the obligation to report may be exempted from the notification obligation to the individual when it demonstrates that “it has implemented **appropriate technological protection measures** [that] … render the data unintelligible to any person who is not authorised to access it.” It is for national competent authorities to assess what the technological measures are appropriate and if they were applied.[29] National competent authorities may issue **guidelines** on and **audit** compliance with the notification obligation.[30] On 24 June 2013 the European Commission has adopted a Commission Regulation [52] (the Regulation entered into force on 25 August 2013), specifying measures applicable to the notification obligation, including the content of notification to the competent national authority and the affected individual or subscriber.

3.5.3.3.2 ENISA Recommendations

In April 2012 ENISA produced Recommendations on technical implementation guidelines of Article 4 ('ENISA data breach recommendations') [52]. Although the scope of the notification obligation is currently (at least, on the EU level) limited to the telecommunications sector, in light of the changes proposed in the draft General data protection regulation to widen the notification scope, ENISA intends its recommendations to be of relevance for all data breach contexts.

The Recommendations propose a systematic approach to personal data breach management, inter alia, by recommending specific steps that the data controller needs to take, with a special importance attributed to the prevention; the appropriate technological and organisational measures, especially those relating to 'data unintelligibility' under Article 4(4) of the ePrivacy directive; recommendations on detection and assessment of the personal data breaches, especially, the methodology to assess the impact and severity of detected personal data breaches. The Recommendations deal with the procedures of notification, notification timing, content and channels of communications [52].

ENISA data breach management approach is based on the existing security incident response management procedures, such as **ISO standard 27035:2011-09(E),** generally involving five steps:

1. Plan and prepare
2. Detect and assess
3. Notify and respond
4. Collect evidence and carry out forensic analysis
5. Review and improve.

As a preventive measure of special relevance under Article 4(3) ePrivacy directive, ENISA, with a reference to the French data protection authority (CNIL), recommends that data is rendered unintelligible when either one of the following apply:

Data has been securely encrypted or hashed:

a) The data was encrypted with a standardised secure symmetric or asymmetric encryption algorithm, or was hashed with a standardised cryptographic keyed hash function.
b) The key used to encrypt or hash the data was not compromised in any security breach.
c) The key used to encrypt or hash the data was generated so that it can- not be guessed by exhaustive key search with current available technological means.

Alternatively, data has to have been securely deleted:

a) It was on a medium that was physically destroyed or
b) It was on a medium that was degaussed or
c) It was deleted with a secure erasure algorithm (DoD, NIST, etc.).

3.5.4 Future European data protection certification after data protection reform

At the moment, the EU data protection framework, including its approach to certification of data protection compliance, is going through a reform process. In January 2012 the Commission

[29] Under Article 4(4), national authorities may issue guidelines regarding the appropriate technological measures.

[30] Article 4 (4) ePrivacy directive

proposed a new Data Protection Regulation ('Commission Proposal'),[31] and in October 2013 the Committee on Civil Liberties, Justice and Home Affairs ('LIBE Committee') adopted its compromise text amending the Proposal ('LIBE compromise text').[32] In order for the Regulation to be adopted, the Council of the European Union has to also approve the changes. Currently, it seems that the Council will postpone its decision to 2015, it is likely that data protection certification will be an important aspect of compliance with future European data protection law.

Provisions of the Commission Proposal relevant for standardization and certification analysis are Article 38 (codes of conduct) and 39 (privacy seals), and Article 18 (data portability).

3.5.4.1 Codes of Conduct (Article 38)

The Commission Proposal continues endorsing codes of conduct and hence, private certification schemes, in Article 38: "Associations or other bodies representing categories of controllers should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors" (Recital 76).

Article 38 specifies the content of the codes and the procedures and gives the Commission the power to decide – upon request of the code 'owners' - on the validity of the submitted codes of conduct.

The LIBE compromise text introduces more clarity into legal status of such codes of conduct, providing that – once a code of conduct receives approval of the Commission - the delegated act of the Commission containing such approval confer enforceable rights to the data subjects. The LIBE text introduces an interesting amendment into the nature of the codes of conduct, providing for an opportunity for the supervisory authorities, in addition to the industry itself, to draw up such codes.

3.5.4.2 Certification: European Data Protection Seal (Article 39)

Article 39 of the Commission Proposal introduces the possibility to establish (multiple) certification mechanisms and data protection seals and marks "in order to enhance transparency and compliance with this Regulation" and enable data subjects "to quickly assess the level of data protection of relevant products and services" (Recital 77). However, the certification mechanism is completely revised in the LIBE compromise text.

The LIBE approach followed the experience of ULD, the Schleswig-Holstein DPA, in introducing a European (both EU- and national-level) certification scheme where data protection authorities are involved.[33] Without eliminating privately operated certification schemes, Article 39 of the LIBE compromise text provides that any controller may request a DPA to certify that data processing is performed in compliance with the data protection legislation, by issuing the "European Data Protection Seal". However, as of 01 January 2014 the ULD will no more operate the EuroPriSe privacy certification scheme, and as the head of ULD, Thilo Weichert, stated " this will allow the program to grow in a way that was not possible as part of a regulatory body like ULD".[34]

The "European Data Protection Seal" – the standardised data protection mark will be issued by the national data protection authorities as opposed to private certification bodies (Article 39(1e)), for a period of no longer than 5 years, registered in an electronic register established by the European Data Protection Board.

[31] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final – 2012/0011 (COD), 25.01.2012.

[32] This section is based on the compromise amendments published by the LIBE Committee of the European Parliament: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf and http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_30-91/comp_am_art_30-91en.pdf.

[33] Independent Centre for Privacy Protection of Schleswig-Holstein, 'Response to the European Commission Consultation on the Legal Framework for the Fundamental Right to protection of Personal Data,' December 2009

[34] https://www.privacyassociation.org/publications/europrise_seal_to_change_hands_january_11.

The certification of compliance with the Regulation is to be performed, for a fee, by supervisory authorities, upon request of either a controller or processor (Article 39(1a)), on a voluntary basis. The auditing of compliance can be outsourced to the accredited, independent and free of conflict of interests, third party auditors (Article 39(1d)), but the final certification is to be performed by the supervisory authority itself. To ensure harmonised certification, the data protection authorities are to cooperate with each other and the European data Protection Board (Article 39(1c)).

In addition, the European Data Protection Board may initiate certification and certify that a data protection-enhancing technical standard is compliant with the Regulation (Article 39(2a)).

3.5.4.3 Data protection seals and principle of accountability

Data protection certification further gains legal significance due to its connection to the newly introduced data protection principle – accountability.

The principle of accountability, articulated by the Article 29 Working Party in its Opinion 3/2010 on the principle of accountability (WP 173),[35] and adopted both by the Commission Proposal and the LIBE compromise text (Articles 5(f) and 22) imposes an obligation on the controller to *adopt* technical and organizational measures to ensure and *demonstrate* – in a transparent manner - that the data processing is consistent with the data protection law. Data protection certification schemes provide the controller with an instrument to comply with the principle of accountability as 'such programs would contribute to prove that a data controller has fulfilled the provision; hence, that it has defined and implemented appropriate measures which have been periodically audited.'[36]

3.5.4.4 Standardisation for data portability

One of the innovations of the Commission Proposal in comparison to the current Data protection framework is a new right to data portability, i.e. a right of a data subject to obtain copy of data processed in an electronic and structured format which is commonly used and allows for further use by the data subject (Article 18(1) of the Proposal).

The Proposal does not refer to a specific interoperable format that would ensure seamless transfer of data from one processing system to another, but empowers the Commission, on its discretion, to specify the respective electronic format, technical standards, modalities and procedures for the transmission of personal data (Article 18(3) of the Proposal).

Article 18 on the right to data portability received a lot of criticism and was deleted in the Parliament text adopted by the LIBE committee in October 2013. Data portability requirements in the Parliament text are combined with the right to access. The data subjects are to have a right to obtain a copy of their data, when processed by electronic means, in an electronic and interoperable format (Art. 5.2a Parliament text). Yet, the Parliament text does not introduce an obligatory requirement to use specific formats.[37]

3.6 Suggested certification approach for FI-STAR

3.6.1 Overall scheme

To provide a simple and effective certification scheme we can suggest a scheme based on Supplier Declaration of Conformity (SDoC) as also compliant by international practice documented in ISO 17050-1 and 17050-2

The different roles can be:

- **Certification authority**: this authority is at the highest level of the project or the FI-PPP programme. It defines the main elements of the certification programme.

[35] Art. 29 Working Party, 'Opinion 3/2010 on the principle of accountability', WP 173, 00062/10/EN

[36] WP173

[37] Gerrit Hornung, A general data protection regulation for Europe? Light and shade in the Commission's draft of 25 Janaury 2012, scripted 9(1), April 2012, p. 74.

- **The Certification body**: this function is an operational one which is only executing the programme, receive the request from suppliers based on SDoC and issue when positive a certificate
- **The candidate** pass all the tests and fullfill all processes as defined by FI-STAR. It submits the SdOC with details to the FI-STAR Certification body

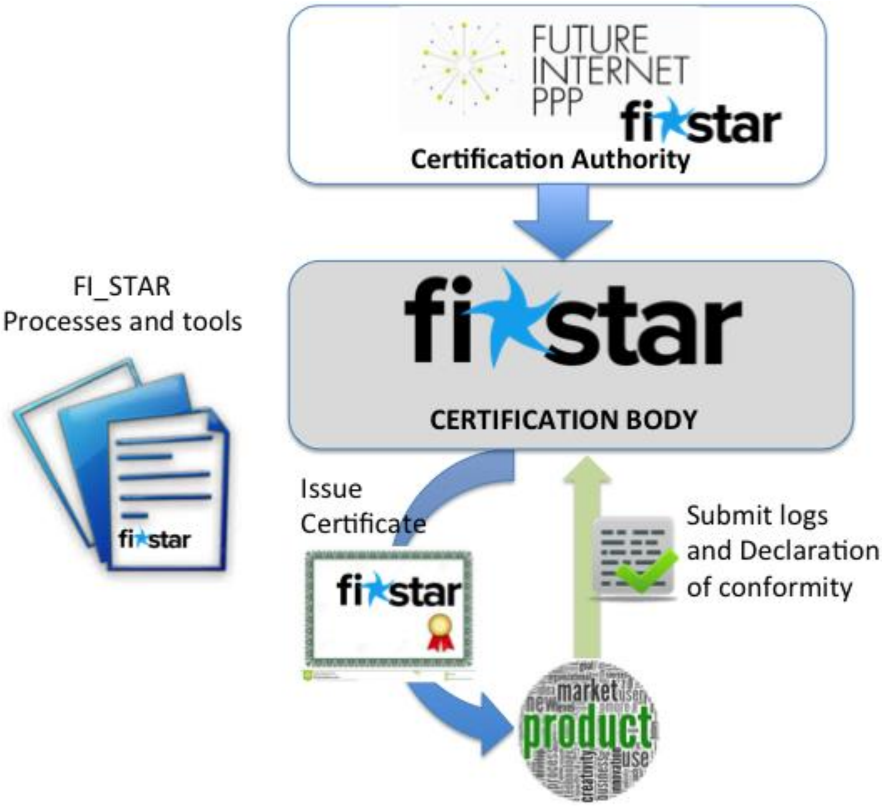
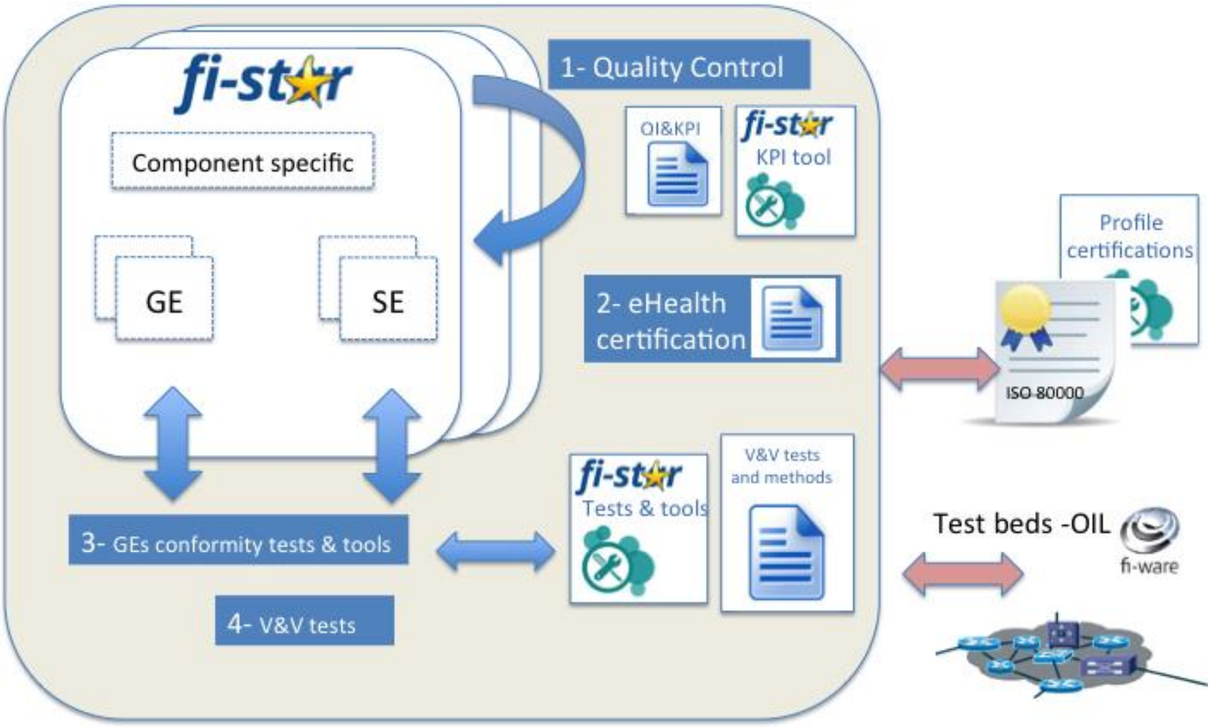


Figure 15: overall certification scheme proposed in FI-STAR.

3.6.2 Certification requirements for FI-STAR components



3.6.2.1 Conformity to FI-PPP elements: GEs, SEs

If a FI-STAR component declared implementing a specific GE or SE, there will two cases

A) a GE or SE tests and tools are available either developed by FI-STAR or available by the community and validated by FI-STAR, in such case the FI-STAR component should pass the tests and prepare the logs to be submitted to the certification board

B) No GE or SE tests and tools are available for a particular GE and SE. In such case FI-STAR will have developed conformity assessment process to be used by the component running at a particular test beds such as XIFI test beds or other available GE test bed. The results of the conformity assessment process should be submitted to the certification board

The test, tools and methods for such tests are described in the deliverable D6.1

3.6.2.2 Quality control

The WP6 defines a quality assessment framework which identifies, in addition to health specific indicators, quality indicators organised in 4 additional thematics:

- Software Verification& Validation (V&V)
- External quality, including users' satisfaction
- End to end delivery
- Sustainability

Fi-STAR components will be evaluated against these dimensions. The different indicators as well as the processes are described in the deliverable D6.1

3.6.3 Certification requirements specific to eHealth

3.6.3.1 Case of eHealth Interoperability Certification

The objectives of the eHealth certification has among several objectives, to promote adoption of a set of recognized standards and profiles, to encourage their implementation and to define certification criteria in order to improve interoperability between systems and to develop a European market. Users will benefit by having a single market of products compliant with the European regulation and with a certain level of Interoperability quality. At the first stage, the EU Commission is today supporting the development of the interoperability framework and in the second stage will support the development of the testing and certification framework. Antilope project by refining the eEIF and proposing a governance of the QL& Certification processes, has been starting to develop such frameworks. Adapted to its own purpose, FI-STAR is one of the candidate for using these frameworks.

Antilope in one of its activities (WP4) describes the functional model and its flexible implementation in Europe and national/regional projects.

In summary, the interoperability certification processes for eHealth should be defined by

- In term of contents:
  - The eHealth European Interoperability Framework, its use cases, the recommended profiles and underlying standards as specifications and requirements that have to be met by the products. For more details, see the Annex A;
  - The test methods. They are based on the existing test methods developed by epSOS, IHE-Europe and Continua Alliance. For more detail, see section 3.3;
  - The test tools that support the eEIF
- In term of organisation:
  - The functional model and the QL& certification processes will be built under the following organisation:
    - A Conformity Assessment schema holder: the role is to specify the QL&Certification scheme including the scope of the certification;
    - The certification body that issues the QL or Certificate;

  - The Conformance Assessments Bodies (CAB): the role is to assess the products. These bodies shall be ISO/IEC 17025 [12].
- In term of consistency and capitalisation among European projects:
  - The European governance shall be defined. It will allow flexibility from European level to national/regional projects and vice versa by using the European testing methods and test tools as a basis. Each project has the ability to extend these tools for their own purposes.

The following schema from Antilope project synthetizes the governance:

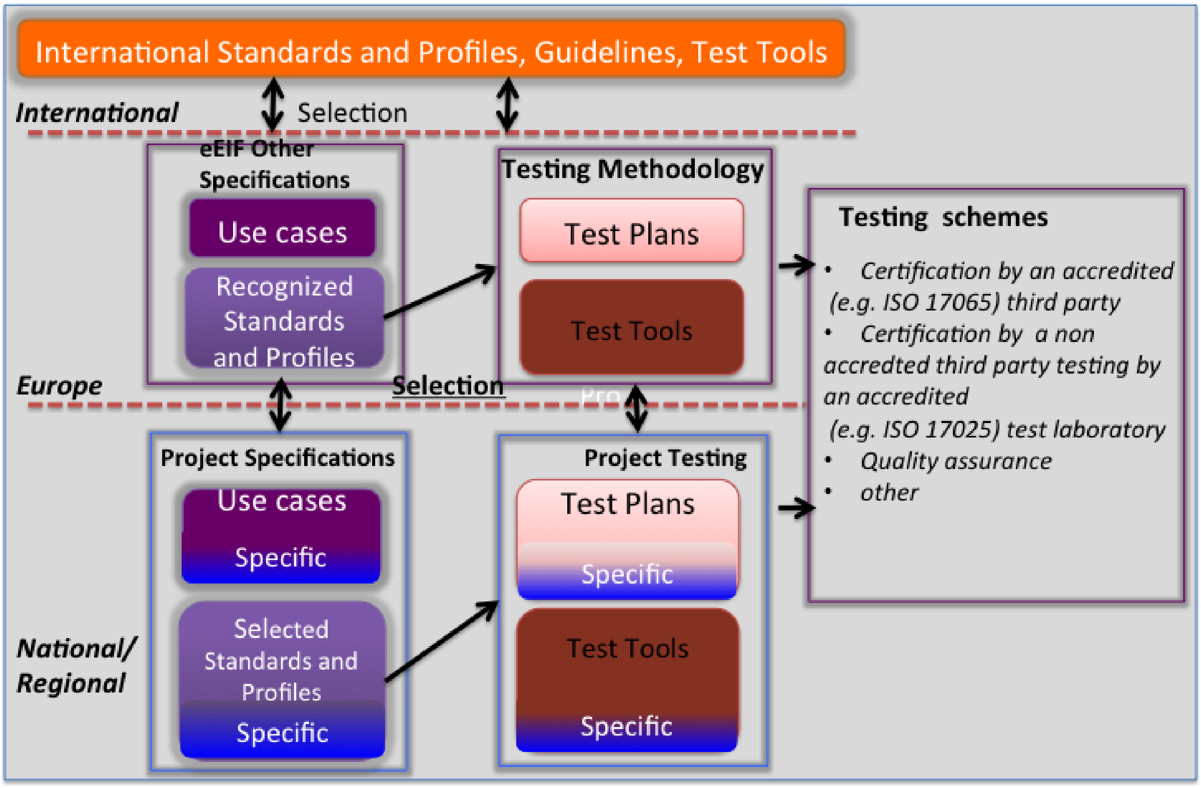

International Standards and Profiles, Guidelines, Test Tools
International
Selection
eEIF Other Specifications
Use cases
Recognized Standards and Profiles
Testing Methodology
Test Plans
Test Tools
Testing schemes
• Certification by an accredited (e.g. ISO 17065) third party
• Certification by a non accredted third party testing by an accredited (e.g. ISO 17025) test laboratory
• Quality assurance
• other
Europe
Selection
Project Specifications
Use cases
Specific
Selected Standards and Profiles
Specific
Project Testing
Test Plans
Specific
Test Tools
Specific
National/ Regional

Figure 16: QL & certification processes (source Antilope project)

3.6.3.2 Certification of Medical Devices

Certification of compliance of the medical devices with safety standards is obligatory. All medical devices except for custom-made or intended for clinical investigations, meeting the essential safety requirements as discussed below must bear the CE marking of conformity when they are placed on the market.[38]

Most of the e-Health solutions developed as a result of FI-STAR will most **likely be medical devices as defined by the European Medical Device Framework ('MDF')** that ensures safety of medical devices brought on the European market, and their free movement in this market. Therefore, they will have to comply with the standardization and certification requirements imposed by the Framework.

The MDF – currently undergoing a reform process[39] - at present is composed of three different directives:

- Council Directive 90/385/EEC on active implantable medical devices (AIMDD),
- Council Directive 93/42/EEC on medical devices ('**MDD**'), and

[38] Article 17 MDD; the devices do not bare CE mark at trade fairs, exhibitions, demonstrations, etc.

[39] On 26 September 2012, the European Commission adopted a Proposal for a Regulation of the European Parliament and of the Council on medical devices and a Proposal for a Regulation of the European Parliament and of the Council on in vitro diagnostic medical devices (http://ec.europa.eu/health/medical-devices/documents/revision/index_en.htm), to replace the existing three directives.

- Directive 98/79/EC of the European Parliament and of the Council on in vitro diagnostic medical devices (IVDD).

FI-STAR use cases do not involve with implantable or in vitro diagnostics technology. The general MDD is of direct relevance for FI-STAR technology. The MDD harmonises basic safety requirements to medical devices across the Member States, both brought on the European market and intended for clinical investigation.

Digital health solutions like software are legally a medical device when they are[40] *"intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application, intended by the manufacturer to be used for human beings' for the purpose of, among others,*

- *diagnosis, prevention, monitoring, treatment or alleviation of disease;*
- *diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap;*
- *investigation, replacement or modification of the anatomy or of a physiological process […].'*

The 'intended purpose' is to be inferred from the information on the labelling, in the instructions and/or in promotional materials.'

The software and other eHealth solutions developed within the FI-STAR project may thus constitute medical devices as defined by the Medical Device Directive ('MDD'). As such, software applications developed will have to comply with the standardization and certification requirements imposed by MDD.

Medical devices may be placed on the European market[41] and/or put into service[42] only if they comply with the quality requirements of MDD, 'when duly supplied and properly installed, maintained and used in accordance with their intended purpose.'[43] Member States cannot disrupt free circulation of such devices within the internal market, as long as they are bearing the **CE mark** under Article 17 MDD, signifying that the device has gone through the procedure of conformity assessment[44].

3.6.3.2.1 Actors involved in CE certification of medical devices

The actors involved in the process of certification of medical devices under the MDD are:

- the manufacturer (or his authorized representative);
- the notified body;
- the competent authority;
- the Commission

The **manufacturer** includes but is not limited to a producer of a medical device. MDD defined the manufacturer as "*the natural or legal person with responsibility for the design, manufacture, packaging and labelling of a device before it is placed on the market under his own name, regardless of whether these operations are carried out by that person himself or on his behalf by a third party*" (Article 1(2)(f) MDD). This definition does not apply to the person who, while not a manufacturer, assembles or adapts devices already on the market to their intended purpose for an individual patient (Article 1(2)(f) MDD, subparagraph 2).

[40] Article 1(2) of MDD. Article 1(2)(g) of MDD"

[41] meaning 'the first [made] available in return for payment or free of charge of a device other than a device intended for clinical investigation, with a view to distribution and/or use on the Community market, regardless of whether it is new or fully refurbished' (Article 1(2)(h) MDD).

[42] meaning 'made available to the final user as being ready for use on the Community market for the first time for its intended purpose' (Article 1(2)(i) MDD).

[43] Article 2 of MDD

[44] Article 4 of MDD

Thus, an institution that outsources the development of a medical app for a smart phone to a third party and brings it out on the market under its name is considered a manufacturer with regard to the app, but not with regard to the smartphone.

An '**authorised representative**' is a natural or legal person established in the EU who "*who, explicitly designated by the manufacturer, acts and may be addressed by authorities and bodies in the Community instead of the manufacturer with regard to the latter's obligations under this Directive*" (Article 1(2)(j) MDD).

The **'notified bodies'** are bodies designated by the Member States to perform conformity assessment tasks (Article 16 MDD), based on the criteria set out in Annex XI MDD. The list of the notified bodies, their identification numbers and "the tasks for which they have been notified", is published and kept up-to-date by the Commission in the Official Journal of the European Communities[45].

When a notified body is involved in the conformity assessment, the manufacturer may apply to **a notified body of his choice** within the tasks for which that body is notified (Article 11(9) MDD).

.The **'competent authorities'** are the national authorities of the Member States. They are endowed with supervisory functions regarding the notified bodies.

3.6.3.2.2 Standards

Before CE certification, **the 'essential requirements'** of safety (specified in Annex I) must be met, taking account of the intended purpose and functions of the devices concerned (Article 3 MDD).

Annex I Essential Requirements contain:

1. General requirements; and
2. Requirements regarding design and construction, more specifically, regarding:
   a. Chemical, physical, and biological properties (Section 7);
   b. Infection and microbial contamination (Section 8);
   c. Construction and environmental properties (Section 9);
   d. Devices with a measuring function (Section 10);
   e. Protection against radiation (Section 11);
   f. Medical devices connected to or equipped with an energy source (Section 12);
   g. Information supplied by the manufacturer (Section 13).

Among other general requirements, if the device is intended for use in combination with other devices or equipment, the whole combination must be safe and not impair the specified performances of the devices.[46] In the case of modular eHealth solutions, this means being tested in combination with all modular components. Mobile apps need to be tested in combination with each smart-phone that it is intended to be used with. This will create difficulties with obtaining a CE mark for software designed to operate on a wide range of devices.[47] To simplify the assessment procedure, the intended use of the smartphone in question should not exclude running eHealth apps. An eHealth app manufacturer may also choose to obtain a CE marking for its software in combination with a particular smartphone or other mobile device.

Devices with a measuring function (such as in the diabetes use case) must be designed and manufactured providing sufficient accuracy and stability within appropriate limits of accuracy and taking account of the intended purpose of the device. The limits of accuracy must be indicated by the manufacturer,[48] etc.

[45] The list is available at http://ec.europa.eu/enterprise/newapproach/nando/index.cfm?fuseaction=na.main

[46] s. 9.1. Annex I of MDD

[47] P. Quinn et al. 193

[48] s. 10.1. Annex I of MDD

Member States shall **presume compliance with Essential Requirements** when a device in conformity with “the relevant national standards adopted pursuant to the harmonized standards[49] the references of which have been publishes in the Official Journal of the European Communities; Member States shall publish the references of such national standards” (Article 5 (1) and (2) MDD).

3.6.3.2.3 Classification of medical devices

In order not to subject all medical devices to the conformity assessment procedures of the same degree of intensity,[50] the following classes of medical devices have been introduced: **Classes I, IIa, IIb, and III.** In June 2010 the Commission adopted guidelines on classification of medical devices.[51]

As the preamble of the MDD explains, classification is based “on the vulnerability of the human body taking account of the potential risks associated with the technical design and manufacture of the devices”. Therefore, **different classes of medical devices necessitate different conformity assessment procedures**:

- For the **Class I** (low risk) devices, the conformity assessment procedures can be as a rule carried out by the manufacturers;
- For **Class IIa**, the intervention of a notified body is compulsory at the production stage;
- For **Classes IIb and III** (high risk), inspection by a notified body is required with regard to the design and manufacture of the devices;
- **Class III** (highest risk) requires explicit prior authorization with regard to conformity before the device is placed on the market.[52]

3.6.3.2.4 Conformity assessment procedures, CE marking

Article 11 MDD prescribes which procedures should be followed to assess conformity with the standards (‘essential requirement’). These procedures vary in intensity according to the type of the device and are described in the Annexes to the Directive.

The conformity with the standards does not always have to be ascertained by CE marking. All medical devices except for custom-made or intended for clinical investigations, meeting the essential safety requirements as discussed below must bear the **CE marking of conformity** when they are placed on the market (Article 17 MDD).

Devices intended for clinical investigation and custom-made devices **do not bear the CE marking**, but still require to go through relevant conformity assessment procedures, as discussed further.

In order to affix CE marking, for **Class III** devices, except for the custom-made devices or devices intended for clinical investigation, **the manufacturer has a choice from:**

- Annex II EC declaration of conformity – full quality assurance procedure; or
- Annex III EC type-examination procedure, coupled with:
  - Annex IV EC verification, or
  - Annex V EC declaration of conformity – production quality assurance procedure.

In case of **Class IIa** devices, except for the custom-made devices or devices intended for clinical investigation, the manufacturer has to follow, either:

- Annex VII EC declaration of conformity procedure, coupled with either:

[49] The harmonized standards include “the monographs of the European *Pharmacopoeia* notably on surgical sutures and on interaction between medicinal products and materials used in devices containing such medicinal products, the references of which have been published in the Official Journal of the European Communities” (Article 5(2) MDD).

[50] MDD Preamble;

[51] European Commission, “Medical devices: Guidance document – Classification of medical devices,” Guidelines relating to the application of the Council Directive 93/42/EEC on medical devices, MEDDEV 2. 4/1 Rev. 9 June 2010, available at http://ec.europa.eu/health/medical-devices/files/meddev/2_4_1_rev_9_classification_en.pdf

[52] MDD Preamble

  - Annex IV EC verification, or
  - Annex V EC declaration of conformity – production quality assurance procedure, or
  - Annex VI EC declaration of conformity – product quality assurance procedure, or
- Annex II EC declaration of conformity – full quality assurance procedure.

In case of **Class IIb** devices, except for the custom-made devices or devices intended for clinical investigation, the manufacturer should follow either:

- Annex VI EC declaration of conformity - product quality assurance procedure (with some limitations); or
- Annex III EC type-examination procedure, coupled with:
  - Annex IV EC verification, or
  - Annex V EC declaration of conformity – production quality assurance procedure, or
  - Annex VI EC declaration of conformity - product quality assurance procedure;

In order to affix CE marking, for **Class I** devices, except for the custom-made devices or devices intended for clinical investigation, the manufacture should follow Annex VII declaration of conformity procedure (Article 11 (5) MDD).

3.6.3.2.5 Special conformity assessment procedures

Conformity assessment of devices for clinical investigation and custom-made devices

Although the devices intended for clinical investigation and custom-made devices do not bear CE marking, their conformity with the specific standards still needs to be ascertained:

Clinical investigation

For the experimental stage of the FI-STAR project, requirements to the devices intended for clinical investigation are of special relevance.

Devices **intended for clinical investigation**, before they are made available to medical practitioners or authorized persons for that purpose, need to meet the conditions laid down in Article 15 and in Annex VIII (Article 4(2) MDD).

Devices intended for clinical investigation are "*intended for use by a duly qualified medical practitioner when conducting investigations* [or any other person who, by virtue of his professional qualifications, is authorized to carry out such investigation] *… in an adequate human clinical environment"* (1(2)(e) MDD).

The **manufacturer** (or his authorized representative) have to:

- follow Annex VIII procedure,
- **notify the competent authorities** of the Member States in which the investigations are to be conducted, by means of a statement (Section 2.2 of Annex VIII).

The **statement** must contain, among others, the clinical investigation plan, the documents used to obtain **informed consent** of subjects, the opinion of ethics committee concerned and details of aspects covered by its opinion, the name of the authorized medical practitioner and institution responsible for the investigations, duration of the investigation and the statement that the device in question conforms to the essential requirements apart from the aspects covered by the investigations and that with regard to these aspects, every precaution has been taken to protect the health and safety of the patient (for a full list of details to be included see Section 2 Annex VIII MDD).

The manufacturer must keep available for the competent national authorities the design and production **documentation** regarding the device in question (under Section 3.2 Annex VIII MDD).

The manufacturer is responsible to take all necessary measures, and must authorize their effectiveness assessment or audit, to ensure that the products manufactured are in accordance with this documentation.

A start of a clinical investigation has to be authorized, and the end of it has to be notified to the competent authority by the manufacturer.

When higher risk devices are concerned (Class III and implantable and long-term invasive devices of Class IIa and IIb), the clinical investigation can only begin in the end of a 60-days period after notification, unless competent authorities decided and notified otherwise (Article 15(2) MDD). The competent authorities may authorize the investigation to begin earlier, upon a positive opinion of an ethics committee.

In other cases, the Member States may issue authorization immediately upon notification, upon a positive opinion of an ethics committee.

Whether the relevant authorizations are by the competent authority differs from Member State to Member State.

Custom-made devices

Custom-made devices before they are placed on the market and put into service, have to meet the conditions laid down in Article 11 in combination with Annex VIII. In case of higher-risk devices (Class IIa, IIb and III), the procedures have to be combined with the statement under Annex VIII, available to the particular patient identified by name, an acronym or a numerical code (Article 4(2) MDD).

National regulation in the Member States may oblige the manufacturers to provide the national competent authority with a **list of custom-made devices** put into services on their territory (Article 11(6) MDD).

Conformity assessment procedure for systems and procedure packs and procedure for sterilization

Of special relevance for FI-STAR modular solutions is a provision concerning systems or combinations of devices. When a device is to be brought on the market as a system or in combination with another device, used within their intended purpose, and all of the devices bare a CE mark, no Article 11 procedures are required, and **a declaration under Article 12 suffices**, where a natural or legal person who brings the system on the market states that:

a) he has verified the mutual compatibility of the devices in accordance with the manufacturers' instructions and has carried out his operations in accordance with these instructions; and
b) he has packaged the system or procedure pack and supplied relevant information to users incorporating relevant instructions from the manufacturers; and
c) the whole activity is subjected to appropriate methods of internal control and inspection.

When such systems or packs of devices bearing CE marking are designed by their manufacturer to be **sterilized before use**, t**he person who sterilizes these before bringing them on the market** should follow, at his choice, either the Annex II or Annex V procedure. These procedures are limited to the aspects of the procedure related to obtaining sterility (Article 12(3) MDD).

These systems or packs do not bear an additional CE marking (Article 12(4) MDD).

In all other cases, e.g. where some devices in the system do not bear a CE marking or where the combination of devices is not compatible in view of their original intended use, Article 11 procedures apply.

3.6.3.2.6 Consequences of non-conformity to the MDD and CE certificate

Suspension or withdrawal and restrictions on a certificate

Under Article 16(6) MDD, if a **notified body** finds that “pertinent requirements of this Directive have not been met or are no longer met by the manufacturer or where a certificate should not have been issued, it shall, taking account of the principle of proportionality, *suspend or withdraw the certificate issued or place any restrictions on it”.*

These sanctions can be avoided if appropriate **corrective measures** are taken by the manufacturer to ensure compliance.

The 'Safeguard clause' and taking off the market

Such devices after the conformity assessment can still be taken off the market by the Member States under the **'safeguard clause'** of Article 8 MDD if - even though correctly installed, maintained and used for their intended purpose - they 'may compromise the health and/or safety of patients, users or, where applicable, other persons.' In order to implement the 'safeguard clause', the Member States establish a system of reporting the incidents of any defects or malfunctions, if they may lead or may have led to a death or a serious deterioration in the health of a patient, user, or any other person, or systematic recalls for the same reasons of the device at hand or a similar device by the manufacturer. Such reporting systems may envisage obligations of medical practitioners or medical institutions to report. All such incidents should be centrally recorded and assessed.

3.6.3.3 Standardization and certification related to medicinal products

The Medicinal products directive[53] ('**the MPD'**) harmonizes requirements towards marketing, procurement, holding, distribution, packaging, labelling and other aspects of supply to the public of medicinal products. Although this Directive is addressed to the member States and needs to be implemented into national law (Article 130 MPD), these requirements can be of relevance to the Leeds use case which is working with distribution of medicinal products, and the Medicinal Products Directive contains requirements to wholesale supply of medicinal products.

These requirements being relevant to only one use case (Leeds) and already managed by local partners, they are not further described in the core part of the document and further details are provided in Annex B.

3.6.3.4 eHealth interoperability requirements for FI-STAR

Three types of use cases have been considered:

- Those that are or willing to be compliant with the eEIF;
- Those have no intention to be compliant and use their own specifications. This situation is not recommended;
- Those are too specific and no existing QL& certification processes are known.

Use cases compliant with the eEIF:

Use cases BPTM, CR, CDTA, DSS and TS are candidates of this category. The table synthetizes the requirements:

Profiles	Sensor (PAN-IF LAN-IF)	Mobile application	Server application	EHR system
Continua guidelines	Continua certification recommended			
IHE Profiles	NA	Connectathon	Connectathon	Connectathon
Project specifications with IHE profiles extensions	Projectathon	Projectathon	Projectathon	Projectathon

[53] Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use OJ L 311, 28.11.2001, p. 67, amended by Directive 2002/98/EC, Commission Directive 2003/63/EC, Directive 2004/24/EC, Directive 2004/27/EC, Regulation (EC) No 1901/2006, Regulation (EC) No 1394/2007, Directive 2008/29/EC, Directive 2009/53/EC, Commission Directive 2009/120/EC, Directive 2010/84/EU, Directive 2011/62/EU, Directive 2012/26/EU.

Three steps on the testing strategy are considered:

- Step 1: the sensors and all the applications that are implemented IHE profiles are invited to pass the IHE Connectathon considering their application roles. Conformity to profiles and workflow test scenarios will be assessed. This testing session is a face to face testing session where developers finalise their development and benefit of the expertise of the other participants.
- Step 2: for each use case, the Projectathon evaluates the conformity to the project specifications including the workflows defined within the use case. The testing session can be a face-to-face session or a virtual session. The data exchanged during this session are dummy data but the environment is set up with all the configurations (OID, UUID, etc.), terminology and coding systems available, dummy patient, dummy documents, etc. Extension or development of test methods and test tools are planned. The projects are the interest to work together in order to reduce the gaps between them and to develop or to ask for development of a set of tools that fit to all projects.
- Step 3: the pre-production testing session: The production environment is in place including the security aspect. Only the exchanged data are not belonging to the real world. The testing session is a virtual testing session.

The schema below synthetizes the testing strategy

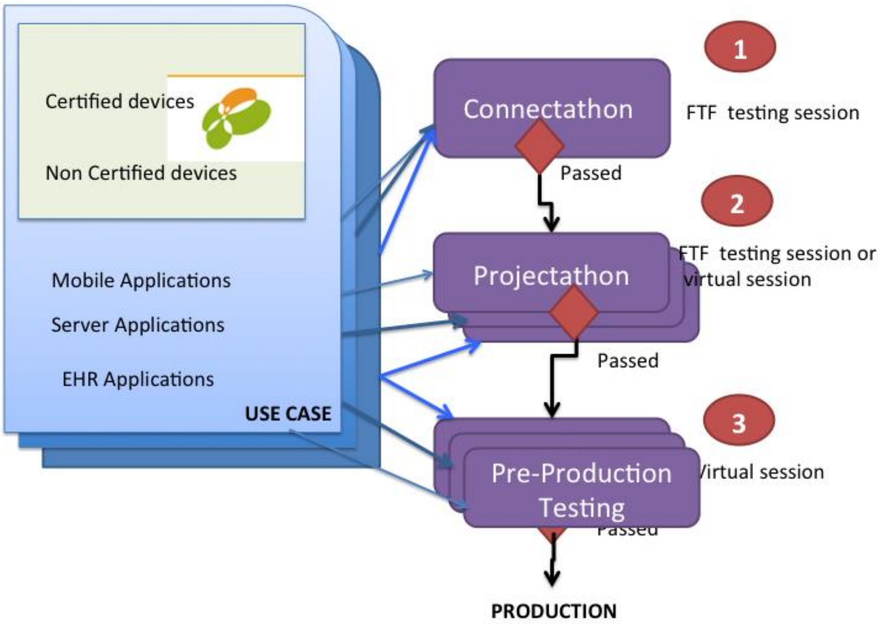


Figure 17: Recommended health certification efforts in FI-STAR

Specific testing strategy

In this case, specific testing tools have to be developed according the project specifications. It is recommended to check if there is any other European project in the same situation. In this case, specifications should be defined as a first draft of future profile within a standard or profile committee (see section 2.4.1. the testing strategy described should be applied.

3.7 Synthesis of proposed validation approach in FI-STAR

The elements gathered during this study allows to define the requirements on standardisation and certification the project would have to comply with. This includes in particular the outlining of a validation and certification strategy for FI-STAR which provides easy and simple proof of compliance to requirements to the market. This strategy needs to be pragmatic while complying with the existing regulatory framework, helping the issuing of high quality and sustainable outcomes by the project FI-STAR and the FI-PPP programme (Figure 18). Three different approaches are then proposed depending on the level of the considered requirements:

- **Regulatory requirements**: there is no other choice than ensuring the regulatory compliance of systems, devices and applications put on the market by the project FI-STAR. Nevertheless, this is usual business of the health IT providers being present in the project and thus does not require project specific attention.
- **External requirements**: these requirements comes from third parties, external to the project and does not contain mandatory requirements of standardization or certification of IT products or IT-based services. Motivation for certification is thus mostly guided by interoperability interests (also here as also promoted as interchangeability and plugability) : FI-STAR developers want to benefit from components (GEs) from the FI-PPP that are in-line with their specification while FI-STAR wishes to develop platforms that are re-useable by third parties (SEs) and which can connect and exchange data with medical systems. In that case, 2 options exist
  - **Validation of GEs/SEs**: this is not provided by any third party today and thus has to be conducted at the FI-STAR level and promoted at the FI-PPP level. This activity is being driven with WP6.
  - **Interoperability with health systems**: many profiles based interoperability schemes and tools are already promoted by many EU projects and Fi-STAR has to capitalize on this important existing offers. It should be conducted on a voluntary basis. For instance Projectathon organised in the framework of connectathon is one of the most efficient way to expose FI-STAR outcome to the health market reality. Such activity has to be done by development teams within FI-STAR with the support of dissemination and exploitation teams. Other offers are developed within the eHealth thematic network Antilope
- **Internal requirements**: while we need to communicate with the external world, we need to be sure what we deliver has high quality and is conform to the expectation (also from users' side). Quality improvement has to be sought to increase the acceptability of FI-STAR outcomes. The project thus has to set its own quality requirements and deploy its internal processes to monitor them. These requirements are described within the quality assessment framework given in D6.1.

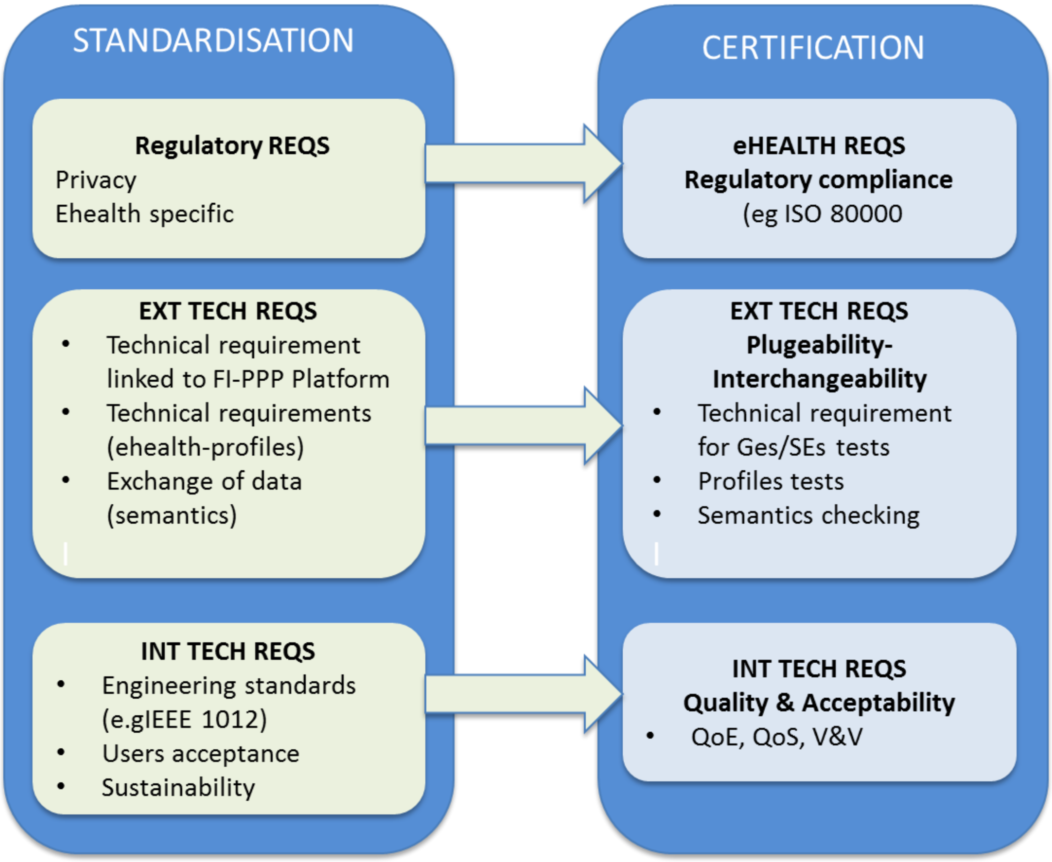


Figure 18: Simplified overview of Standardisation and Certification requirements in FI-STAR

4 Conclusion on Standardisation and Certification requirements

The deliverable D1.2 “Standardisation and Certification requirements” analysed the current standardization and certification landscapes in the fields related to FI-STAR activity. These are focused on IT development for health applications within the FI-PPP program.

Listing of standards relevant to eHealth in the context of FI-STAR has been done. Getting through the certification required to conform to national and EU regulations (mostly based on ISO 80001, ISO 13485, ISO 27000) is left to the professional health IT system developers of the consortium, as part of their usual activities.

Focus is rather positioned on eHealth interoperability through the use of eHealth interoperability profiles such as the one defined by IHE. Profiles of interest for FI-STAR use cases have been identified and discussed with the use cases. The validation of eHealth interoperability of FI-STAR platforms and applications during connectathon events is encouraged. This should not only be managed by technical WPs but also has to be supported by dissemination and communities engagement activities of the project, as a way to tighten the links of FI-STAR with the health community.

Regarding data protection, the EU Data Protection Directive does not contain mandatory requirements of standardization or certification of IT products or IT-based services. Nevertheless, the specific case of health data management is treated as part of the standards mentioned above

The interactions of FI-STAR toward the FI-PPP required more attention as not being managed by any third party outside FI-STAR. Close relations have to be maintained between FI-STAR and the FI-PPP to develop a validation process for enablers produced by the FI-PPP as well as FI-STAR. This approach has to be disseminated and promoted to the FI-PPP architecture board.

Finally general standards related to software development practices have been identified. While their use is not an obligation, it is recommended to include them as part of the overall project processes and monitor their use within the project quality assessment framework deployed in WP6.

References

[1] http://www.fi-star.eu/

[2] FP7-ICT-2009-4 HITCH- Healthcare Interoperability Testing and Conformance Harmonization Grant agreement no.: 248288

[3] eHealth-INTEROP Report in response to eHealth Interoperability Standards Mandate, SA/CEN/ENTR/000/2007-20 eHealth Mandate M/403-Phase 1, 10 February 2009, http://www.ehealth-interop.eu.xx

[4] ETSI White Paper No. 3, “Achieving Technical Interoperability - the ETSI Approach”, H. Van der Veer and A. Wiles, 2008.

[5] https://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/Standardization_Plan/Standardization_Needs

[6] https://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/Standardization_Plan/Standardization_Gap_Analysis

[7] http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/Standardization_Plan/Strategy

[8] “Machine to Machine Communications (M2M); Study on Semantic support for M2M Data”, DTR/M2M-00017, ETSI TR 101 584.CIP-ICT PSP TN EHRQTN Certification of HER Systems Grant agreement no.: 238912

[9] CIP ICT-PSP 2010/4 Pilot type A epSOS Smart Open Services European Patients Grant agreement no.: 224991 - www.epsos.eu

[10] Article 29 Working Party in Opinion 02/2013 on apps on smart devices adopted on 27 February 2013 (‘WP 202’)

[11] ENISA, ‘Information security certifications. A Primer: products, people, processes’ Deliverable 2.1.5/2007, p. 11

[12] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN(2013) 1 final, 7/2/2013, (last accessed on 23.09.2013), available at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667

[13] Competitiveness and Innovation Framework Programme, ICT Policy and Support Program, ICT-PSP/2009/3, **Annex I, Description of Work, Renewing Health**, REgioNs of Europe WorkINg toGether for HEALTH, Grant agreement no.: 250487,Version 9, 18 January 2010.

[14] IHE Integrating the Healthcare Enteprise : www.ihe.net

[15] Wikipedia

[16] Continua alliance : www.continuaalliance.org

[17] CIP-ICT TN Antilope- adoption and take up of standards and profiles for eHealth Interoperability Grant agreement no.: 325077 - www.antilope-project.eu

[18] European Commission – ISA work programme – eHealth European Interoperability Framework (eHealth EIF). Framework contract N° DI/06691-00. 4 documents

[19] ISO/IEC 17000 – Conformity Assessment – Vocabulary and general principles

[20] ISO/IEC 1702 – General requirements for the competence of testing and calibration laboratories

[21] GITB – Global eBusiness Interoperability Test Bed methodologies (http://www.ebusiness-testbed.eu)

[22] http://www.eurorec.org

[23] http://www.healthit.gov/policy-researchers-implementers/meaningful-use-stage-2

[24] ISO/TR 16982:2002 Ergonomics of human-system interaction -- Usability methods supporting human-centred design

[25] IEC 62304:2006 Medical device Software --- Software life cycle processes

[26] EOTC flyer to present CE marking , New & Global approach

[27] Medical Device Directive 93/42/EEC of June 1993 concerning medical devices: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:EN:PDF

Directive 2007/47/EC of 5 september 2007 aminding council Directive 90/385/EEC on the approximation of the laws of the Member States relting toactive implantable medical devices, Council Directive 93/42/EEC concerning medical devices and Directive 98/8/EC concerning the placing of biocial products on the market : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:247:0021:0055:EN:PDF

Proposal for a regulation of the European parliament and of the council on medical devices and amending directive 2001/83/3C, regulation (EC) N°178/2002 and reguklation (EC N°1223/2009: http://ec.europa.eu/health/medical-devices/files/revision_docs/proposal_2012_542_en.pdf

[28] http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/default.htm

[29] Directive 1995/46/EC, Official Journal 1995, L281/31.

[30] Ronald de Bruin, Ewout Keuleers, Christophe Lazaro, Yves Poullet and Marjolein Viersma, ‘Analysis and definition of common characteristics of trustmarks and web seals in the European Union. Final Report’, V2.3 February 2005, p. 38

[31] The Report to the Information Commissioner’s Office names two European-wide codes of conduct: the International Air Transportation Association (IATA) and the Federation of European Direct and Interactive Marketing (FEDMA) (Robinson et al, pp. 9-10).

[32] LRDP KA TOR Ltd and Centre for Public Reform, ‘Comparative Study of Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments. Final Report submitted to the European Commission ’, 20 January 2010, p. 53.

[33] https://www.datenschutzzentrum.de/faq/guetesiegel_engl.htm

[34] LRDP KA TOR Ltd and Centre for Public Reform, ‘Comparative Study of Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments. Final Report submitted to the European Commission ’, 20 January 2010, p. 54.

[35] http://www.cnil.fr/la-cnil/labels-cnil/

[36] Rowena Rodrigues, David Wright, and Kush Wadhwa, ‘Developing a privacy seal scheme (that works)’ in International Data Privacy Law, 2013, Vol. 3, No. 2, p. 100

[37] Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability, available online at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf (last accessed on 23.10.2012).

[38] Study on EU privacy seals, JRC/IPR/2012/G.7/00013/OC, http://web.jrc.ec.europa.eu/callsfortender/index.cfm?action=app.tender&id=1764

[39] https://www.european-privacy-seal.eu/about-europrise/fact-sheet

[40] Kirsten Bock, ‘Final Report’, EuroPriSe project, Deliverable R08, WP1

[41] LRDP KA TOR Ltd and Centre for Public Reform, ‘Comparative Study of Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments. Final Report submitted to the European Commission ’, 20 January 2010, p. 53

[42] https://www.european-privacy-seal.eu/criteria/

[43] Independent Centre for Privacy Protection of Schleswig-Holstein, ‘Response to the European Commission Consultation on the Legal Framework for the Fundamental Right to protection of Personal Data,’ December 2009

[44] Kirsten Bock, ‘Final Report’, EuroPriSe project, Deliverable R08, WP1

[45] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. OJ L 13, 19.1.2000, p. 12–20

[46] Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council [Official Journal L 175, 15.7.2003], http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003D0511:EN:NOT

[47] ENISA "Smartphone Secure Development Guideline": http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines.

[48] Directive 2002/58 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31/07/2002 P. 0037 - 0047) (‘ePrivacy directive’).

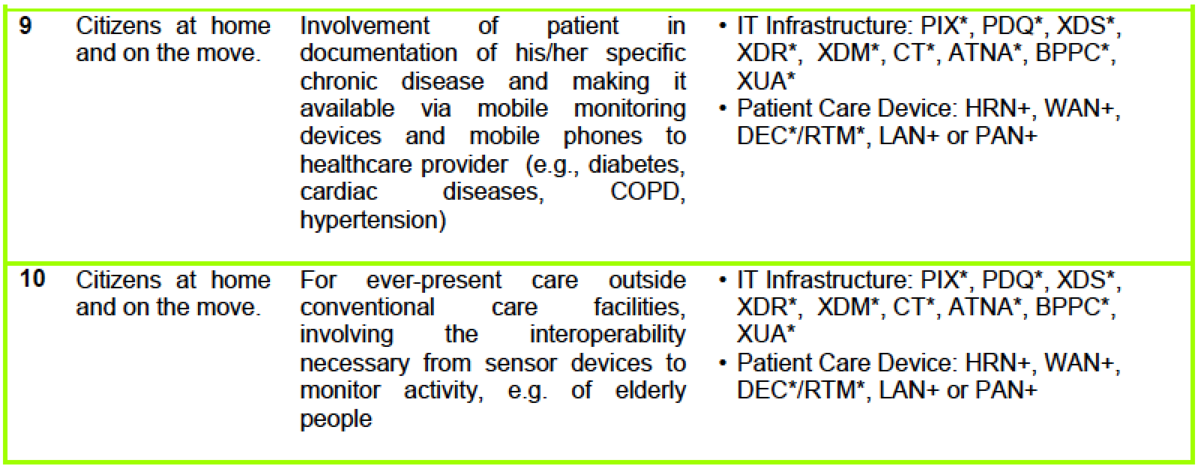
[49] Patrick Kierkegaard. 2011. ‘Electronic health record: Wiring Europe’s healthcare’, in Computer Law and Security Review, 27. p. 512

[50] Commission Regulation No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications.

[51] Available online at http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn

[52] ENISA Data breach recommendations, p. 9

Annex A Use Cases and Profiles from the eEIF [10]



9	Citizens at home and on the move.	Involvement of patient in documentation of his/her specific chronic disease and making it available via mobile monitoring devices and mobile phones to healthcare provider (e.g., diabetes, cardiac diseases, COPD, hypertension)	• IT Infrastructure: PIX*, PDQ*, XDS*, XDR*, XDM*, CT*, ATNA*, BPPC*, XUA* • Patient Care Device: HRN+, WAN+, DEC*/RTM*, LAN+ or PAN+
10	Citizens at home and on the move.	For ever-present care outside conventional care facilities, involving the interoperability necessary from sensor devices to monitor activity, e.g. of elderly people	• IT Infrastructure: PIX*, PDQ*, XDS*, XDR*, XDM*, CT*, ATNA*, BPPC*, XUA* • Patient Care Device: HRN+, WAN+, DEC*/RTM*, LAN+ or PAN+

Annex B Standardization and certification related to medicinal products

The Medicinal products directive[54] (‘**the MPD’**) harmonizes requirements towards marketing, procurement, holding, distribution, packaging, labelling and other aspects of supply to the public of medicinal products. Although this Directive is addressed to the member States and needs to be implemented into national law (Article 130 MPD), these requirements can be of relevance to the Leeds use case. The Directive aimed at “the adoption of the same standards and protocols by all the Member States [that] will enable the competent authorities to arrive at their decisions on the basis of uniform tests and by reference to uniform criteria and will therefore help to avoid differences in evaluation”[55].

‘Medicinal products’ defined as: “*(a) Any substance or combination of substances presented as having properties for treating or preventing disease in human beings; or (b) Any substance or combination of substances which may be used in or administered to human beings either with a view to restoring, correcting or modifying physiological functions by exerting a pharmacological, immunological or metabolic action, or to making a medical diagnosis”* (Article 1(2) MPD).

In particular, Title V of the Directive contains requirements to labelling and package leaflet and Title VII contains requirements regarding wholesale distribution and brokering.

‘Wholesale distribution of medicinal products’ refers to “*[a]ll activities consisting of procuring, holding, supplying or exporting medicinal products, apart from supplying medicinal products to the public. Such activities are carried out with manufacturers or their depositories, importers, other wholesale distributors or with pharmacists and persons authorized or entitled to supply medicinal products to the public in the Member State concerned” (*Article 1(17) MPD*)*

These activities are subject to **distribution authorization** by the Member States (Article 77 MPD). The **minimum requirements** in order to obtain a distribution authorization are set out in Article 79 and 80 MPD and include:

- suitable and adequate premises, installations and equipment, to ensure proper conservation and distribution of the medicinal products;
- the applicant must verify that the medicinal products received are not falsified by checking the safety features on the outer packaging;
- the applicant must have staff, and in particular, a qualified person designated as responsible, meeting the conditions provided for by the legislation of the Member State;
- the applicant must undertake to fulfil the obligations of a holder of the distribution authorization, i.e.:
- they must make the premises, installations and equipment referred to in Article 79(a) accessible at all times to the persons responsible for inspecting them;
  - obtain their supplies of medicinal products only from persons who are holding the distribution authorization or who are exempt from obtaining such authorization;
  - supply medicinal products only to persons who are themselves in possession of the distribution authorization or who are authorized or entitled to supply medicinal products to the public in the Member State concerned;
  - verify that the medicinal products received are not falsified by checking the safety features on the outer packaging;
  - importantly, distribution authorization holders must have an **emergency plan** which ensures effective implementation of any recall from the market;

[54] Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use OJ L 311, 28.11.2001, p. 67, amended by Directive 2002/98/EC, Commission Directive 2003/63/EC, Directive 2004/24/EC, Directive 2004/27/EC, Regulation (EC) No 1901/2006, Regulation (EC) No 1394/2007, Directive 2008/29/EC, Directive 2009/53/EC, Commission Directive 2009/120/EC, Directive 2010/84/EU, Directive 2011/62/EU, Directive 2012/26/EU.

[55] Recital 11 MPD

- keep records either in the form of purchase/sales invoices or on computer, or in any other form, containing at least the following details for any transaction in medicinal products received, dispatched or brokered: date, name of the medicinal product, quantity received, supplied or brokered, name and address of the supplier or consignee, as appropriate, batch number of the medicinal products.
- keep these records available to the competent authorities, for inspection purposes, for a period of five years;
- comply with the principles and guidelines of good distribution practice for medicinal products (Article 84 MPD);
- maintain a quality system setting out responsibilities, processes and risk management measures;
- immediately inform the competent authority and, where applicable, the marketing authorisation holder, of falsified medicinal products they receive or are offered.

Title VIIa harmonizes the requirements regarding **sale of medicinal products at a distance to the public,** containing mainly information obligations.

Annex C New term of reference of standardisation and validation working group suggested by FI-STAR

C.1 Standardisation & Validation Working group

The main objective of the Standardisation and Validation Work Group (WG) is to facilitate the projects in the identification of existing and potentially applicable standards and in the process of standards definition from pre-standardisation to compliance testing and marketing, and help maximise the outcome of the Future Internet PPP. A first goal of this WG is to provide advice about existing standards that can be used in a FI-PPP project, when the project requires it. Another objective is to ensure that projects and developments are correctly implementing existing standards and that new standards can be validated wherever feasible. Standards aim to ensure interoperability and such goal can be achieved only if there is clear identification of conformity to standards process we called here ”validation” The leader of this WG will be assigned by the SB.

In particular the activities are carried out within the CONCORD task 3.3 which includes the coordination and support of pre-standardisation activities, in the Working Group on Technical Alignment and Standardisation which is a shared activity of T1.3 (Architecture Board and Liaison) and this task. The objectives of the Technical Alignment and Standardisation Working Group are to agree on a common roadmap across projects towards the development, use and validation of the FI-PPP platform, and to facilitate the FI-PPP projects in the identification of opportunities for open standards. The common roadmap will ensure the efficient and effective interaction between Architecture Board, FI-WARE and Use Case projects. As regards standards, projects will be facilitated in the process of standards definition from pre-standardisation to compliance testing and marketing, thus helping to maximise the outcome of the Future Internet PPP.

A fundamental guiding principle in the work of this WG is first and foremost to find an existing standard that can be used for the purposes of the FI-PPP project at hand. The specific goals of the WG are to help the projects identify existing world-class standards, educate the projects as to the terminology, processes and challenges relating to standardization, identify the gaps between existing standards and standards that need to be created in order to achieve the expected impact, help identify the need for agreeing upon new standards in underdeveloped areas, and help the standard owners to create, market and maintain those standards, preferably under the auspices of well-established standards-setting organisations (SDO’s). The leader of this EG will be assigned by the Steering Board.

Table 5: Pre-standardization, standardization and validation actions and policy

STGW vs. other initiatives	Standardisation at UC level	FI PPP STGW level
Pre standardisation	• Preparation of individual standardisation plans • Standardisation topics at UC level • Vertical White paper to introduce project scope • Identify SDO and standard to address.	• Starting from individual standardisation plan, to provide a programme level vision • To assess isolated and common standardisation topics • Preparation of white paper encompassing more UC on same vertical sector and technologies • Support action about SDO identification • IPR issues

Standardisation	• Approaching SDO • Participate and contribute to standardisation proposals • Actions at partner level, normally • Follow partner level standardisation policies	• When needed, facilitation actions can be made in approaching SDO • End of phase2 mainly
Validation	• Contribute to developing conformity to standards specifications • Contribute to validate new standards • **Contribute to Validation and inter-operability of FIWARE GEs** • **Assessment of GEs validation**	• Defining validation methodologies to ensure conformity to standards • Defining validation methodologies to validate new standards (e.g. interoperability events) • Defining validation programme to ensure confidence

C.2 Activities related to the Generic Enablers (GEs)

The UC projects of phase 2 have been conceived to strongly base their architectures on the open GEs available from FI-WARE core platform. Therefore an important pre-standardisation activity, that shall be included in this WP, will be the validation and test of GEs included in the UCs. This will give the possibility to the entire FI PPP to identify specific needs and new requirements for the GEs and eventually the identification of new topics for the standardization that will be enforced and proved during the validation and inter-operability tests with other solutions and GEs included in the scenarios of the UCs. In addition to these vertical pre-standardisation activities, it is also possible that direct GEs standardization contributions will be generated by UCs in the frame of FI-WARE plan. Meaning that, GEs standardization plan of FIWARE could progress together with some UC proposals from the beginning even before the execution of GEs validations.

As there are now many available GEs and more and more users, there will be a danger that standards/specifications are not enough validated (e.g. limited number of level of interpretation by implementers) and that the way of checking conformity to standards, if left to the market forces, will create different non interoperable implementations. Therefore it is of utmost importance that (new) standards (here meaning standards, specifications and all used in the context of the definition of a GE) are also developed to define clear rules and tests to prove conformity to standards. The level of complexity in the definition of such new standards, the methodology to be used and the final process to check conformity to standards should be discussed at the level of programme in the Standardisation and Validation WG.