FI.ICT-2011-285135 FINSENY

D.7.1 v1.0

First set of consolidated ICT Requirements to the Architecture Board

Contractual Date of Delivery to the CEC: Month 6 (*30.09.2011)*	
Actual Date of Delivery to the CEC: Month 6 (*15.10.2011)*	
Author(s):	*Martin N. Wagner Neumann*
Participant(s):	*ATOS, NSNG, SIEMENS, BAUM, EDF, ESB, ENG, EON, EAB, EDD, EUTC, FIR, ORANGE, GRENOBLE INP, IBE, SWP, SYNELIXIS, TID, VTT, TSSG*
Work package:	*WP 7: Consolidation*
Estimated person months:	*20*
Security:	**PU** = Public
Nature:	**R (R** = Report, **P** = Prototype, **D** = Demonstrator, **O** = Other**)**
Version:	1.0
Total number of pages:	262

Abstract:
The aim of the project FINSENY is to design advanced smart energy scenarios and use cases in five different areas of the smart energy landscape (Distribution, Microgrids, smart buildings, electric vehicles management and electronic marketplace for energy). The latter scenarios have to use extensively the generic enablers that will be implemented by Future Internet Core Platform (FIWARE project), in order to plan for attractive pilots.

The first step was the specification of the scenarios and use cases which has been implemented in the dedicated Work packages (WP2-WP6). The second step was the extraction from the latter of the ICT requirements described as Internal Reports.

This deliverable documents the overall **first set of consolidated ICT requirements.** To do this, the FI-PPP AB requirement templates and methodology was followed. From now on, requirements will be inserted and refined at the Source Forge site of FIWARE and discussed in the AB.

D7.2 (M16) will document the final consolidated requirements from FINSENY.

Keyword list:

FI-PPP, FINSENY, Future Internet, FI-WARE, Smart Energy Grid (SEG), Distribution Network, Building Block (Use Case), ICT Requirements, Functional ICT Architecture, Microgrid, Smart Buildings, Electrical Vehicles, Electronic Marketplace for energy

Disclaimer: Not applicable.

Executive Summary

Future Internet technologies are playing a critical role in the development of Smart Energy infrastructures by enabling new functionality while reducing costs. And these new features are the result of the analysis of scenarios and requirements that support them; therefore one of the most relevant objectives for the FINSENY project is identify, describe, consolidate and share the ICT requirements of Smart Energy Systems from the view point of the use of the Future Internet core platform services and infrastructure that is being designed in the FI-WARE project, activities that are performed by WP 7 – Consolidation.

The objective for the **WP7 – Consolidation** is the assembly of the results from the scenario WPs (2- 6), the analysis and evaluation of the ICT requirements and the organization of the interaction with the other FI-PPP use case projects, FI-WARE as well as INFINITY trial planning.

Consequently, the activities performed until now in order to document the requirements available in this deliverable can be summarized as follows:

1st Step: Specification of the FINSENY scenarios and Use Cases performed by WP2 to WP6.

2nd Step: Derive and Specify the ICT Requirements related to the Use Cases and describe them as Internal Reports for the WP7.

3rd Step: Consolidate the ICT Requirements and send them to the Architecture Board.

The current document, consolidates (e.g. filters, eliminates duplicates, improves descriptions, etc.) the lists of requirements produced individually in Work Packages 2 to 6. The document is composed of the following sections:

- The description of the methodology and templates used during the process.
- A Summary Section for the Use Cases and ICT Requirements identified by WPs 2 to 6.
- Templates (filled) used to consolidate and to report the ICT requirements to AB (Annex I and Annex II).

It is important to highlight that during the first phase of the scenario specification, the latter were conceived from the viewpoint of the final users of each and every energy landscape areas handled in FINSENY (see below the WP short descriptions). Therefore the ICT requirements at this stage capture only general aspects related to ICT already organized in different functional categories.

From now on, the scenarios will be refined in order to be decomposed in a way that they will incorporate the use of FI-WARE chapters and enablers. Therefore the actual requirements will be further elaborated in an iterative process, interacting with FI-WARE through the AB and by using the Source Forge tool that has been released in September 2011.

A short description of the WPs that contribute with the Use Cases and the ICT Requirements in this deliverable is:

- WP2 defines the ICT solutions for reliable and efficient operation of future Smart Distribution Networks taking into account large share of Decentralized Energy Resource services and flexibility of the grid.
- WP3 identifies the ICT solutions to efficiently monitor and control Microgrids and their interconnection to the larger grid.
- WP4 addresses ICT solutions for intelligent energy management for buildings and the interfaces to relevant market players.
- WP5 considers the necessary ICT infrastructure to support large scale charging of plug-in electrical vehicles.
- WP6 studies ICT solutions for a future electronic market place for energy and the interfaces to the various market players.

Authors

Partner	Name	Phone / Fax / e-mail
ATOS		
ATOS	Martin N. Wagner	Phone: +34 91 214 8227 e-mail: martin.2.wagner@atosresearch .eu
NSN		
NSN	Werner Mohr	Phone: +49 172 8224826 e-mail: Mohr.Werner@nsn.com
	Holger Elias	Phone: +49 172 8224826 e-mail: Holger.Elias@nsn.com
SIEMENS		
	Kolja Eger	Phone: +49 89 636 42215 e-mail: kolja.eger@siemens.com
	Jürgen Götz	Phone: +49 89 636 40733 e-mail: juergen.goetz@siemens.com
ENG		
	Giusi Caruso	Phone: +39-06-83.07.46.65 Fax: +39-06-83.07.44.08 e-mail: giuseppa.caruso@eng.it
	Pasquale Andriani	Phone: +39-06.83074313 Fax: +39-06-83.07.44.08 e-mail: pasquale.andriani@eng.it
FIR		
	Jonas Fluhr	Phone: +49 241 47705 508 e-mail: jonas.fluhr@fir.rwth-aachen.de
GRENOBLE INP		
	Didier Boeda	Phone: +33 (4) 76 82 63 61 Fax: N/A e-mail: Didier.Boeda@g2elab.grenoble-inp.fr e-mail:
Thales Communications		
	Lionel Besson	Phone: +33 1 46 13 24 90 e-mail: Lionel .BESSON@fr.thalesgroup.com
TID		
	Pierre Plaza	Phone: +34 914832826 Mob: +34 63829278 e-mail: pierre@tid.es
VTT		
	Henryka Jormakka	Phone: + 358 40 511 6275 Fax: +358 20 722 7028 e-mail: henryka.jormakka@vtt.fi
	Timo Kyntäjä	Phone: +358 40 178 3487 e-mail: timo.kyntaja@vtt.fi

Table of Contents

List of Figures

Index of Tables

1. Glossary of Terms

The glossary of terms used in this deliverable can be found in the public document Glossary Terms v2.2.doc also available at http://www.fi-ppp-finseny.eu/. Specific terms and abbreviations used in this deliverable can be found in Chapter **Error! Reference source not found.**.

2. Introduction

Deliverable **D7.1 - First set of consolidated ICT requirements to the AB** documents the methodology and templates used to consolidate the ICT Requirements compiled from the different scenarios and provided to the Architecture Board.

The objective for the **deliverable** is to document the consolidation process of the results from the scenario WPs (2-6) by analyzing and evaluating the ICT requirements described in the Internal Reports prepared by the Use Cases WPs and report the results as a first set of ICT Requirements to the Architecture Board of the FI-WARE project.

To meet the objective for the deliverable D7.1 WP2 to WP7 performed the following activities executed sequentially:

- **1st Step: Specification of the FINSENY scenarios and Use Cases performed by WP2 to WP6.**

  This step has identified in each of the Work packages 2 to 6, relevant scenarios in the Smart Energy domain that will make extensive use of the Future Internet. These scenarios were conceived from the smart energy landscape insights perspective, analyzing the stakeholders and use cases that are relevant in the smart energy domain. The results are documented on the DX.1 deliverables of the above Work packages.

- **2nd Step: Derive and Specify the ICT Requirements related to the Use Cases and describe them as Internal Reports performed by WP2 to WP6.**

  These Internal Reports gather the 1st set of ICT requirements gathered by the FINSENY project. The process is based on the previously specified scenarios and use cases that are presented in the project deliverables DX.1.

  The Internal reports include an analysis of the defined Reference Scenarios and the outlaying Building Blocks were performed, producing different requirements that are categorized and described.

- **3rd Step: Consolidate the ICT Requirements and send them to the Architecture Board performed by WP7.**

  The first activity was to determine a Template for Requirements to:
  - Clarify any ambiguity related to classifications.
  - Define the scope of the template carefully.
  - Avoid unintelligible assumptions.
  - Involve ALL WPs from the beginning.
  - Agree collectively in a template format that suites all scenario needs and specificities.

  Once the template was agreed, the subsequent activities were directed to consolidate the ICT Requirements by grouping them first based on a division in two main categories:

  - **General and component requirements:** contains mainly subcategories that are common to many ICT systems, e.g. interoperability, scalability, reliability, availability, physical media, future-proof system, and environmental requirements. To properly manage the sub-categories a categories layers list were prepared to group them.
  - **Functional and technical requirements**: lists subcategories from more functional point of ICT systems: Performance, QoS, service orientation, management, usability, and security.

  Finally, teams were identified to strengthen the requirements according to their characteristics and to finally integrate the results into a single template. This allowed the staff to meet the reporting needs for the ICT requirements defined by the AB.

The requirements themselves are documented in more detail in two separate Excel-Files; one for FINSENY consolidation purposes and another to report the ICT Requirements to the Architecture Board. Since the requirement analysis just started, further requirements are presumably to be discovered and existing ones elaborated on during the next months to meet the FI-WARE chapter and enabler Backlog and development process.

Tools and templates are useful to support the requirements engineering process. Within the FINSENY project, WP 7 provides a standardized template to retrieve and manage requirements to all Work Packages as an Excel-File. Moreover, the Architecture Board has also provided their own Excel template to receive the ICT Requirements resulting from the Use Case Project of the FI-PPP. WP7 template follows very closely the latter.

Although the use of two different templates requires additional work for conversion and alignment, FINSENY decided to keep both updated in order to ensure the greatest amount of information available for the next phases of the project. In order to quickly get the first set of ICT requirements the task leaders of WP 2 to WP 6 provided a reduced version of the FINSENY template, which is used in this document.

The consolidation process of the found requirements made obvious that many requirements can be derived from more than one use case and that it is crucial to find the right level of detail. Important questions were and will be asked throughout the consolidation phase, the most relevant ones at this stage were those concerning particularity and generality of the recorded requirements. The most important task was to classify the requirements eliminating duplicates, inconsistencies and common related ICT areas in which the requirements could lie.

Work on this topic is just in the early stages and has to be continued.

In order to create generic and specific ICT enablers, the identified requirements, need to be broken down to a lower level of granularity and consolidation efforts need to be enforced. At the same time, new requirements might appear during future discussions.

Finally, a brief description of each WP will allow understanding more clearly the scope and complexity of the consolidation process carried out (see Figure 1: FINSENY Work Packages):

- WP2 defines the ICT solutions for reliable and efficient operation of future Smart Distribution Networks taking into account large share of Decentralized Energy Resource services and flexibility of the grid.
- WP3 identifies the ICT solutions to efficiently monitor and control Microgrids and their interconnection to the larger grid.
- WP4 addresses ICT solutions for intelligent energy management for buildings and the interfaces to relevant market players.
- WP5 considers the necessary ICT infrastructure to support large scale charging of plug-in electrical vehicles.
- WP6 studies ICT solutions for a future electronic market place for energy and the interfaces to the various market players.

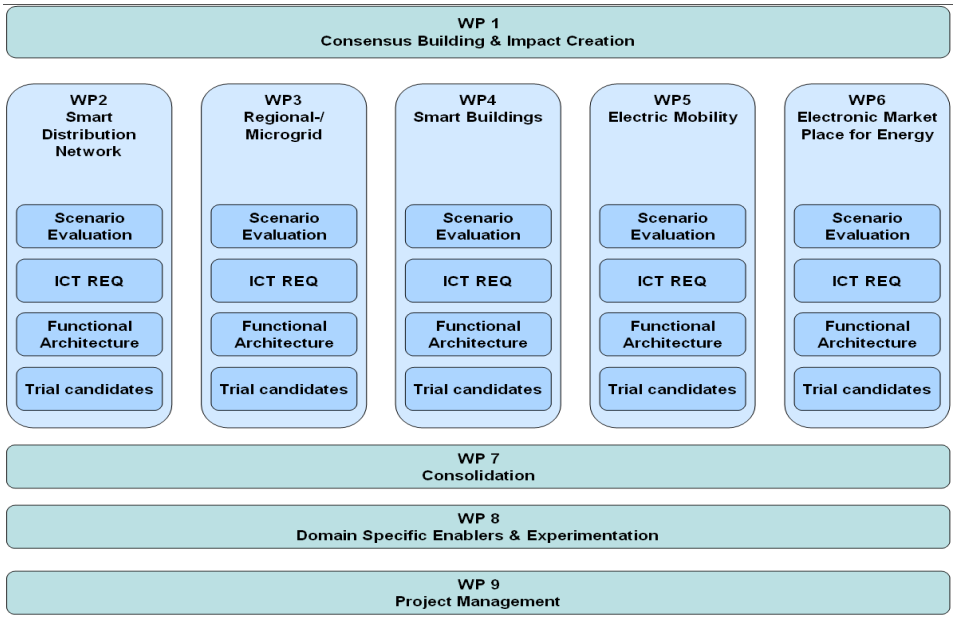

Figure 1: FINSENY Work Packages

The vertical Work Packages cover the five scenarios which gain most from the use of ICT in the future Smart Energy landscape. Each Work Package follows a similar methodology in building the specific scenarios from various building blocks (Use Cases) identifying prominent ICT requirements, describing possible solutions and subsequently scenario specific trial plans.

The transversal Work Packages deal with topics that are relevant for several or all scenarios, consolidate the results from the different scenarios and provide the contact points to other projects:

- WP1 is the instrument to ensure coherence of the technical, business and market related activities of the project by providing the technology frame work for the scenarios, examining the research landscape, standardization, regulation and evaluating major cross-cutting topics (i.e. Security). It is also responsible for the dissemination and exploitation of the project results.
- WP7 consolidates the requirements from the scenarios and identifies the common enablers together with the technology platform and the other usage area projects. It will further select and describe the trials for the second phase based on the input from the vertical WPs and WP8. A continuous interaction with the vertical WPs will assure a coordinated approach and consistent functional ICT architectures. This will be organized by the Project Management Team (PMT) and the Technical Manager (TM).
- WP8 develops domain specific enablers in order to support requirements which are not covered by the common enablers. A proof of concept will be done for the most relevant domain specific enablers.
- WP9 is responsible for the overall project management.

Consequently **D7.1 – First set of consolidated ICT Requirements to the Architecture Board (AB)** is the result of performing the 3 Steps as described before. The document is composed of the following sections:

- The description of the methodology and templates used during the process.
- A Summary Section for the Use Cases and ICT Requirements identified by WPs 2 to 6.
- Templates (filled) used to consolidate and to report the ICT requirements to AB (Annex I and Annex II).

This initial work is based on existing knowledge on the selected Building Blocks (Use Cases) and the resulting ICT Requirements don't cover all ICT aspects of DNs as each building block is considered individually and for example aspects concerning the parallel processing of the building blocks are not considered yet.

This will be done for the final version of the ICT requirements in parallel and interaction with the definition of the Functional ICT architecture which will also take such aspects into account. The ICT requirements will be used for the definition of common and domain specific enablers within FI-WARE and FINSENY and it is expected that they are also contributed to the ongoing European Smart Grid standardization activities (CEN/CENELEC/ESI Smart Grid Coordination Group) for the definition of standardized functions and protocols for the Smart Grid.

3. Overview of the FINSENY Methodology

The FINSENY Project developed its own methodology to extract and analyze the ICT Requirements from the Use Cases but the FINSENY Methodology has taken into account the following documents:

- IntelliGrid Methodology for Developing Requirements for Energy Systems.
- Recommendations for the Description and Management of Use Cases for Smart Grids developed by Deutsche Kommission Elektrotechnik Elektronik Informationstechnik (DKE).

Other relevant documents related to requirements methodologies reviewed and analyzed were:

- Towards a Goal-Oriented Requirements Methodology Based on the Separation of Concerns Principle
- Security Quality Requirements Engineering (SQUARE) Methodology
- PDM: A requirements methodology for software system enhancements
- PlasTEP - Standardisation and requirements: Methodology for comparison
- Agile Requirements Modelling in Requirements Engineering

Each and every one of these documents were analysed and evaluated from the perspective of the Consolidation of ICT requirements and all have had an impact on the methodology described in this chapter.

But most important was IntelliGrid Methodology for Developing Requirements for Energy Systems with Recommendations for the Description and Management of Use Cases for Smart Grids as a document validator of the results to be achieved. Consequently the next two sections below describe the foundations of these documents.

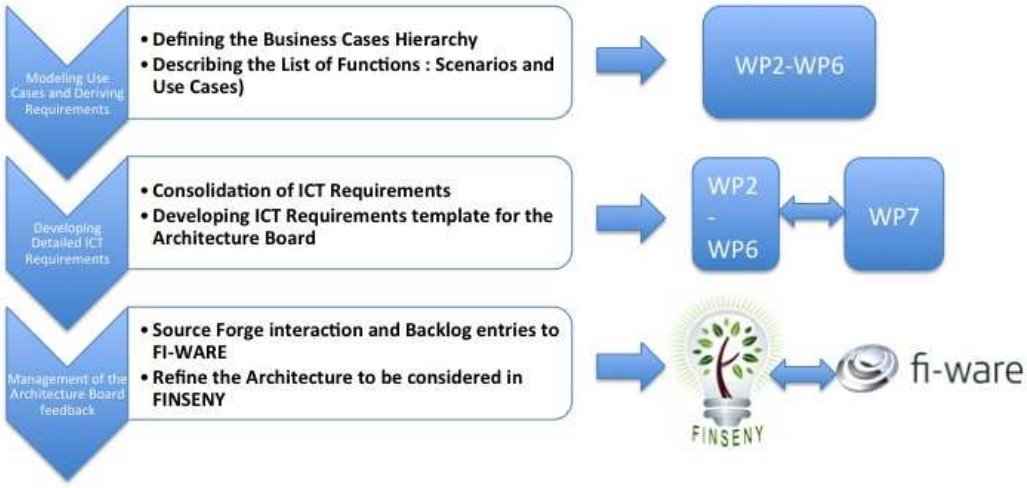

Figure 2: Requirement elicitation Methodology in FINSENY

3.1 Methodology fundaments

3.1.1 IntelliGrid Methodology for Developing Requirements for Energy Systems

3.1.1.1 Objectives of this Specification

As defined by the IEC, the scope of IEC TC8 is to "prepare and coordinate, in co-operation with other TC/SCs, the development of international standards and other deliverables with emphasis on overall system aspects of electricity supply systems and an acceptable balance between cost and quality for the users of electrical energy. Electricity supply system encompasses transmission and distribution networks and connected user installations (generators and loads) with their network interfaces."

IEC TC8 is therefore developing this Publicly Available Specification (PAS) with the following objectives:

- To develop a standard methodology for determining and defining user requirements in a consistent and comprehensive manner. Standards often address only the technical issues that are included in technical specifications; however, it is just as vital to develop standards to assist users to clearly and comprehensively define their requirements.
- To clarify the distinction between "user requirements" (the "what" as needed by power system experts) and "technical specifications" (the "how" as technical descriptions of systems, applications, and information flows to meet the "what"). Currently this distinction is an "invisible line" so that often the "what" and the "how" are mixed together – with technology-oriented project engineers jumping directly to the "how" without fully exploring the "what" with the power system experts.
- To emphasize the critical need to determine all user requirements first, before any commitments are made on "how" to meet those requirements. Because automation and control systems are so complex and are becoming increasingly so, if all requirements are not clearly defined first, then the premature design of systems can block or seriously hinder meeting those requirements that were not initially recognized.
- To provide a means for testing the systems once implemented to ensure that the user requirements are truly met, regardless of what standards and technologies are ultimately incorporated by the vendors.

3.1.1.2 Scope of the Specification

This Publicly Available Specification (PAS) defines a methodology for power system domain experts to determine and describe their user requirements for automation systems, based on their utility business needs. This methodology was originally developed as part of the IntelliGrid Architecture developed by the Electrical Power Research Institute (EPRI), as a means to implement the "IntelliGrid vision" of the automated, self-healing, and efficient power system of the future.

3.1.2 Recommendations for the Description and Management of Use Cases for Smart Grids

Deutsche Kommission Elektrotechnik Elektronik Informationstechnik (DKE)

This document take into account the complexity of the smart grid especially because of the variety of actors and systems and details recommendations to develop use case descriptions that could be used to create a common understanding and for the development and identification of interfaces and data models. From the point of view of DKE, the identification of needs for standardization play a decisive role in addition to the objectives stated above.

In this context, use case descriptions are to be established for various target groups, such as companies in the energy industry, IT manufacturers, equipment manufacturers, standardization organizations, legislators, and companies from other sectors than the energy industry.

In order to master the challenges associated with the compilation and management of use cases, it is recommended that the process is structured by implementing of the following measures:

- Use of conventions: Guidelines, for example, of naming conventions and particular UML diagrams for the presentation of graphics.
- Limitation to the essentials: Avoidance of redundancies, for example, and reduction to relevant information only.
- Use of familiar/proven methods/approaches: Relying, for example, on familiar/proven modeling languages such as UML.
- Tool support: Use of software tools to reduce manual work, especially for quality and consistency assurance.

Requirements for technical process support

Additionally the document describes the method to assist the activities of use case identification, processing and by information technology to ensure rapid and consistent processing and demand-driven management and analysis facilities. A technical solution should therefore cover these functions of identification and processing, management and use.

- Functional requirements

The technical solution should enable recording of the text of the use cases, structured in accordance with the extended IEC/PAS 62559 [6] template. Apart from the text, integration of graphical representations (e.g. UML diagrams) at the locations provided in the template should also be possible.

- Non-functional requirements

Together with the requirements stated in the previous section, non-functional requirements which have an effect on the handling of the system and on its behaviour are also to be taken into account.

The support tool should be easy to use and intuitively understandable, and should only require a shallow learning curve, as the aim is to give as many people as possible the opportunity to contribute their ideas to the standardization work.

Furthermore, cultural and political requirements are to be taken into account; the Enterprise Architect tool, for example, is used for IEC standards 61968/61970, which makes it advisable to provide an export function to this tool or aim for an implementation using it. With regard to the contribution of the use cases to be compiled with the tool, multilingual support is also desirable as it could lead not only to greater use of the use cases compiled but also to a larger group of users for use case compilation and import.

3.2 Management of ICT Requirements

A goal is a high-level objective that the Use Case under consideration should achieve. In turn, an ICT requirement is a description of a system service or constraint needed by a Use Case to achieve a goal. So, an ICT requirement specifies how a goal should be accomplished by a proposed system.

Besides the services and the quality restrictions that a system should provide, an ICT requirements also should include the application domain information and the organizational context where the system will be applied. From this point of view, we can identify three types of requirements: functional, non-functional and organizational requirements. It is important to distinguish the types of requirements since they have different characteristics and therefore, by means of this distinction, we can choose the adequate methods and techniques that should be used during ICT Requirements process.

The traditional approaches used in software development are driven by functional requirements and their focus is on achieving the desired functionality of the system. However, a broader view of software development is one that goes beyond the description of system functionalities, also including organizational and non-functional requirements in a requirements specification.

3.2.1 Functional Requirements

Functional requirements (FRs) capture the intended behaviour of the system in terms of services, tasks or functions the system is required to perform. This kind of requirement is generally specified by means of inputs, processing, outputs, controls, exceptions and entities. The more common techniques for specifying functional requirements are: use cases, scenarios, data flow diagrams and state transition diagrams. Currently, use case is the most used practice to capture and represent functional requirements, especially in object-oriented software development.

A use case describes a set of interactions between actors and the system necessary to deliver the service that satisfies the user goal. It also includes possible alternative sequences that may satisfy the goal, as well as sequences that may lead to failure in completing the service because of exceptional behaviour, error handling, etc.

3.2.2 Non-Functional Requirements

Non-functional requirements (NFRs) are requirements that impose restrictions on the product being developed (product requirements), on the development process (process requirements), or they specify external constrains that the product/process must meet (external requirements). These constraints usually narrow the choices for constructing a solution to the problem.
The distinction between functional and non-functional requirements may cause confusion. Some NFRs characteristics are used to distinguish them from functional requirements:

- NFRs are focused on how the software must perform something instead of focused on what the software must do.
- NFRs “cross-cut” software functionality.
- NFRs express constraints or conditions that need to be satisfied by functional requirements and/or design solutions.
- Different from functional requirements that can fail or succeed, NFRs rarely can be completely met: their satisfying is accomplished within acceptable limits.

Most approaches to systematically deal with non-functional requirements focus on specific NFRs such as security and performance. In turn, the NFR Framework can be applied to a variety of non-functional

requirements. In this approach, NFRs are treated as soft goals to be satisfied by means of operationalization's (operations, data representations, architectural decisions, etc.).

Although non-functional requirements are crucial for system development success, they are seldom analyzed and, even when they are considered, they are generally poorly documented:

1. They are often stated in requirements specifications just as abstract, vague and informal declarations such as: "the system should have good security, performance, confidentiality, usability". This kind of declaration makes it difficult to analyze and to verify how to meet the non-functional requirement. Moreover, it may be ambiguous since different interpretations about the real meaning of the NFR are possible. For those reasons, we advocate that abstract declarations of NFRs need to be broken down into smaller components and then converted into operationalization's that together contribute for achieving these NFRs.
2. Normally, non-functional requirements are not documented in a specific artefact. On the contrary, they are declared repeatedly in each functional artefact affected by them. This fact contradicts the separation of concerns principle and, consequently, the requirements comprehension, evolution and reuse are damaged.

3.2.3 Prioritize ICT Requirements

In most cases, the Use Case Projects will be unable to implement all of the ICT requirements due to lack of time, resources, or developing changes in the goals of the project. Therefore, the purpose of this data is to prioritize the ICT requirements so that the FI-WARE can choose which ICT requirements are relevant and in what order. Thus, the categorization of the ICT Requirements is crucial for prioritization.

The available prioritization methods are flexible and can be as simple as unstructured deliberation between the Use Case WP but for the FI-PPP related projects the Architecture Board defines the prioritization values as follows:

- **MUST** - Features that absolutely have to be done are categorized as "Must". If any of these features are not done, the project will be considered a failure.
- **SHOULD** - Features that are important to the success of the project, but are not absolute musts (they have a workaround or will not cause the project to fail) are categorized as "Should".
- **COULD** - Features that are nice to have but are not core features are categorized as "Could".
- **WON'T** - Features that are not going to be implemented this time are marked as "Won't".

Therefore the FINSENY project decided to handle 2 different priorities, one related to the priority of the ICT Requirements to the project itself and the other one that will depends on the feedback to be received from FI-WARE project.

4. ICT Requirements of Work Package 2 to 6

4.1 WP2 – Distribution Network

All smart grid solutions rely on the Distribution Network so this must be seen as a key enabler for any future improvement in efficiency, safety and sustainability of the energy supply. However, any improvement in the Distribution Network will be very expensive because its size is huge, including thousands of primary substations, hundreds of thousands of secondary substations, tens of millions of grid user connections in each European Country.

4.1.1 WP2 Use Case Summary

4.1.1.1 Mobile Work Force Management (MWFM)

It covers the ability for field crews to have access to work orders in the field. The main issue about this UC is to use pervasive means of communication options especially in case of disturbance of regular communication.

4.1.1.2 Fault Location, Isolation and Service Restoration (FLIR)

This building block (UC) describes the procedures after a fault until the service is restored. It includes the identification of a fault, determining its location, isolating the faulty section and reconfiguring the grid to re-energize these sections as quickly as possible.

4.1.1.3 MV DAC from utility control Centre (MVDAC)

Data Acquisition and Control of real and non-real time information of MV electrical network from the utility control Centre. The differences from the already deployed HV or VHV DAC are the size of the network (more than 100 times bigger) and the location of the controllable elements which are closest to the customers.

4.1.1.4 SG Energy Control of Power Inverter (SGEC)

This use case describes the interactions, mechanisms and the interfaces of power inverters in context of a smart grid. Power consumption from the grid as well as power infield into the grid is considered.

4.1.1.5 Dynamic Control of Active Components (DCAC)

This building block (UC) covers the dynamic control (performed automatically) of distributed active network components on substation level with the goal to ensure stable and energy efficient network operation.

4.1.2 Summary of WP2 ICT Requirements before Consolidation

WP2 ID	Name	Category	Short Description	Priorities
1	Interoperability on IT (Server) level	Interoperability	Interoperability on - North-bound IT I/Fs between DSO, Aggregator and VPP wrt process and application data and database formats - South-bound IT I/Fs wrt device information models	MUST
2	Interoperability on IT (Server) level 2	Interoperability	Interoperability between - Central Dispatch System IT I/Fs and - Field Mobile Devices (Smart Phone or/and laptop) wrt process and application data and database formats utilizing various communication links	COULD
3	Interoperability on Communications Technology (CT) layer	Interoperability	Interoperability on - North-bound CT I/Fs between DSO, Aggregators and VPPs wrt intra and inter-company communication - Standardized South-bound I/Fs wrt SG-devices communication	MUST

4	Interoperability on Communications Technology (CT) layer 2	Interoperability	Interoperability on Communication Technology (CT) layer requires utilization of any useful link available under disturbed operating conditions.	COULD
5	Time Synchronization	Interoperability	Today the Internet does not show any deterministic behaviour. However, within a smart grid measurement values are transported which could require a fast transport (e.g. phase measurements). Also alarm signals sent out by components should arrive to the components´ controller with low latency. In order to achieve this the following methods could be applied: In case of scheduled actions a time based planning of the communication could further optimize the communication load within the communication network, as there are (in ideal case) no collisions will occur. This could be achieved by setting up a planning of telegram slots. The control of the components in the grid is then done using a time-slot-controlled data-/telegram transfer. It would be enough to reserve some slots for the above mentioned cases (alarm, high dynamic measurement values). The necessary number of reserved channels depends on the MTBF of the network (because the number of alarms relates to the MTBF). In case that planning is not set in place a time-stamped telegram could be used in order to interpret e.g. metering data in a more precise way. However, that method is maybe not good enough for alarms. But in both cases the deterministic of the communication network is enhanced. Reserved time-slots are normally realized by synchronization of all time-bases which are present in the various components of the grid. That synchronization could be done on various ways. One way is to use the time signals which are spread via satellites or terrestrial broadcast.	MUST
6	Scalability on IT (Server) level	Scalability	Scalability of the IT systems and their I/Fs to allow for system expansion	MUST
7	Scalability of Networks	Scalability	Scalability of communication networks connecting - North-bound IT I/Fs (Enterprise Bus) between DSO, Aggregators and VPPs incl. intra and inter-company connections - South-bound IT I/Fs to SG-devices	MUST
8	Scalability on IT (Server) level and Communications Technology (CT) layer	Scalability	Scalability of the IT (central and mobile) systems to allow for system application and I/F-type expansion between Central Dispatch System (CSD) and Field Mobile Devices (FMD).	COULD
9	Reliability and availability on IT (Server) level	Reliability and availability	Reliability of IT operations towards Aggregator, VPP or DSO processes, applications, databases and SG-devices.	MUST
10	Reliability and availability on Communications Technology (CT) layer	Reliability and availability	Reliability of CT layer I/Fs towards Aggregator, VPP or DSO and SG-devices.	MUST

11	Handover Management	Reliability and availability	The communication handset device used by field worker to synchronize work orders should have the availability to manage the handover between several commutations media in a transparent way. The best media should be selected regarding the QoS needed in term of latency, jitter and bandwidth. In case of a crisis situation (a tempest for example), a crisis media (such as Private Mobile Radio) should be available for data communication with the same handset device used by workers during “normal” situation.	SHOULD
12	IP mobility	Reliability and availability	From the Dispatch System point of view, the communication system must be able to “push” data to the worker handset whatever the telecommunication medium the worker is currently using, even if its IP address has changed.	SHOULD
13	Adaptation of application to available bandwidth	Reliability and availability	If a low bandwidth media is used (for example in the case of a crisis situation after a tempest), the central IS Dispatch System must adapt its response according to the bandwidth available: only the core data of the work order are sent and not the attached files.	SHOULD
14	Scheduled actions	Reliability and availability	Scheduled actions are to be used to transmit automatically a pre-defined set of data to and/or from the power site (eg. power inverter) without sending messages for ordering that data in before. Such data could be regular status information, metering data, meteorological data, etc. If the transmission time is not deterministic a time-stamp should be part of the transmission.	SHOULD
15	Failsafe Mechanisms	Reliability	As stated in the power inverter use-case description, the inverter can have different communication partners (TSO, DSO, Aggregator, Virtual Power plant ...). However, just one communication partner (“Controller”) is allowed to control the inverter, but several communication partners could be simultaneously informed about the status of the inverter and/or additional information like metering and/or forecast data. From this the communication links and the kind of information to be transported need to be enabled between the inverter and the relevant communication partners in a flexible way. However, in case the “controller” went into an error-state and is unable to continue sending valid control-signals to the power-inverter, the communication watchdog (built-in the inverter) would automatically shut-down the power-inverter after the projected watchdog-time is over. In that case the complete power feed into the grid would be lost immediately, which could result in further shut-downs within the grid. From this there must be installed a fast mechanism which enables a fast take-over of the control task by another “controller” in order to continue power processing by the inverter. Of course, not only the control task must be shifted, but also all relevant data necessary to perform the controller function.	MUST
16	Backup of communication links	Availability	Backup solution should be provided for the communication links. Interfaces enabling communication should operate also at the time when the DSO grid is down. Exception can be a LV PLC link.	COULD

17	Single point of failure avoidance	Availability	It should be assured (to the most possible extend) that if a component fails, it fails in a manner that does not impact other parts, nor generate unnecessary traffic on the ICS, nor cause another problem elsewhere, such as a cascading event, which would affect other parts and functions. If that cannot be assured a backup/redundancy for the component has to be provided.	COULD
18	Dedicated or Shared Transport Infrastructure	Physical Media	Control from an Aggregator, VPP or DSO needs appropriate transport network capacity, which may be supplied by a dedicated operator on an exclusive or shared basis	MUST
19	Dedicated or Shared Transport Infrastructure 2	Physical Media	The Communication Technology (CT) layer requires utilization of any useful link available under disturbed operating conditions. This may be supplied by a dedicated operator on an exclusive or shared basis	COULD
20	Telco Infrastructure	Physical Media	Control from an Aggregator, VPP or DSO needs appropriate transport network capacity, which may be supplied by a Telco operator	COULD
21	Telco Infrastructure 2	Physical Media	The Communication Technology (CT) layer requires utilization of any useful link available under disturbed operating conditions. This may be supplied by a Telco operator.	COULD
22	Future-proof system design requirements	Future-proof system	Future-proof system design wrt to modularity, standardization, maintainability and HW/SW upgradeability	MUST
23	Persistent data storage	Future-proof system	SG devices must contain enough non-volatile memory (e.g. flash memory) for storing measurements, internal data, and enable future firmware and software updates.	MUST
24	Environmental Requirements for Information and Communication Technology	Environmental	Communication equipment for SG-field-devices / Field Mobile Devices and IT (Servers) operated reliably under different environmental conditions.	MUST
25	Availability in end points	Performance	Availability in end points	COULD
26	Availability in central points	Performance	Availability in central points	COULD
27	System availability	Performance	Non critical components: 99.5% + availability System-critical components: 99.9% +	COULD
28	Maximum Time to Repair (MTTR)	Performance	Maximum Time to Repair	COULD
29	Mean Time Between Failures (MTBF)	Performance	Mean Time Between Failures	COULD
30	Latency	Performance	The communication infrastructure must offer a guarantee on the maximal round trip time for messages (from the application on the originator device to the destination device and back)	COULD
31	Delay and Jitter	Performance	Delay and Jitter must be controlled for Telecontrol Function	COULD
32	Bandwidth	Performance	Bandwidth requirements for MV secondary substations	COULD
33	Bandwidth allocation	Performance	Bandwidth ~ 100 kbps	COULD
34	Packet Loss	Performance	Packet Loss for MV secondary substations	COULD
35	Batteries Autonomy	Performance	All ICT elements that provide Telecontrol function must have a Battery that isolate them from the power supply	COULD

36	QoS – networks	QoS	Every network (or network part) should be able to manage differentiated services through the management of priority levels. Instead of DiffServ e.g. MPLS label switch path protocols can be used.	COULD
37	QoS – applications	QoS	Relevant applications may be implemented using priority aware libraries.	SHOULD
38	High priority asynchronous messages	QoS	In case of alarms, e.g. in conjunction with power inverters, the according asynchronous messages must be transported very fast to the controller, as alarms normally reflects a very soon loss of energy production. In order to further guarantee the stability of the smart grid, therefore, this information must be transported with highest priority or via reserved communication channels. Without time-synchronization just the priority of the (asynchronous) telegram can be used to reduce the latency from submitting the message until receiving it.	MUST
39	Service discovery mechanism to set appropriate CoS for communication	Service oriented approach	A service discovery mechanism needs to be specified and implemented in order to set the communication network CoS according to the SG-devices´ communication requirements.	MUST
40	Communications network management	Management	The devices of the system shall support a network management system (NMS) e.g. SNMP and MIB for network information management. The management system should provide visualization of the status of all network elements for easy overview of the whole network.	MUST
41	Data management	Management	The use case involves handling (processing, analyzing, semantically classifying and accessing) large volumes of data that partially have to be stored for later use (e.g. billing, planning, historical analysis, regulation). The data must be kept consistent and synchronized with other systems within seconds. Data consistency has to be executed by DMS/SCADA system	MUST
42	Data values checking	Management	The use cases involve monitoring and otherwise retrieving large amounts of data from different parts of the distribution network. The data integrity ensures that there is no tampering with the data but still there could be problems e.g. with sensors. Malfunctioning devices of the SG could produce data that should not be accepted by the receiving entity. This can be considered as a certain kind of sanity check, but it can also be utilized with fault detection procedures. This is a requirement for the application level of the SG system software.	MUST
43	Remote configuration	Management	The network management system should support remote configuration of the equipment. Remote reset of the devices should be available. Remote SW updates of substation and devices shall be possible.	MUST
44	Grid operator interface	Usability	The display (HMI) of the grid control application to the grid operator has to be clear and intuitive, providing maximum usability, as it may be used in stressing situations. In case of Demand Side Management, the tariff/price information received from the network has to be understandable both by the automatic home/building energy management system and by the customer (person)	MUST

45	Authentication and authorization	Security	System components shall uniquely authenticate users and specific components before establishing a connection. The components shall enforce separation of duties through assigned access authorization. The user privileges should be restricted to only those that are required for each person's role, taking into account emergency cases. In situation of emergency user rights override option should be always implemented by providing higher priority than security/access control.	MUST
46	Data backup and recovery	Security	Backups of critical software, applications, and data for all components of the SCADA system should be assured. Backup should be all data and applications needed to replace failed components within a reasonable period of time as required to satisfy regulatory requirements and to restore the system to normal operation. Backups shall be physically separated from the operational components. Synchronization of the backup and operating data must be assured.	MUST
47	Data confidentiality	Security	It shall be possible to ensure the confidentiality of the communicated data by cryptographic mechanisms, unless otherwise protected by alternative physical measurements. The latency introduced from the cryptographic mechanism shall not degrade the functionality of the system.	MUST
48	Data integrity	Security	It shall be possible to ensure the integrity of the communicated data and to verify whether the data hasn't been tampered. The latency introduced from the protection mechanism shall not degrade the functionality of the system.	MUST
49	Non-repudiation	Security	It shall be possible to prove that information has been send by a specific source.	MUST
50	Malicious code protection	Security	The smart grid system shall employ malicious code protection mechanism. The protection mechanisms shall be deployed in such a manner as to limit the impact of the attack to a small geographical area prior to detection and eradication.	MUST
51	Intrusion detection	Security	The system shall detect the anomalous events (e.g. meter data alerted) within the network boundaries.	MUST
52	Denial-of-service protection	Security	The system should restrict the ability of internal or external users to launch denial-of-service attacks against the network components.	MUST
53	Cryptographic Key Establishment and Management	Security	Cryptographic protection and key management infrastructure shall be selected. The selection should match the value of the information being protected and the protected system operating constraints.	MUST

Table 1: WP2 ICT Requirements Summary

4.2 WP3 - Regional -/ Microgrid

The Microgrid scenario has been chosen as an important and visionary electricity grid scenario to analyze ICT requirements. Microgrids are essentially a substructure of the global grid and comprise local low-voltage and even medium-voltage distribution systems with distributed energy resources and storage devices in order to satisfy the demands of energy consumers. Such systems can be operated in a semi-autonomous way, if interconnected to the grid, or in an autonomous way (islanding mode), if disconnected from the main grid.

4.2.1 WP3 Use Case Summary

- **Business Use Cases**

4.2.1.1 Microgrid Operator sells and buys energy on the external markets

In this use case, the Microgrid Operator acts as an aggregator for all his contracted prosumers inside the Microgrid. He negotiates contracts with his customers (consumers) to represent them towards the (external) wholesale market. Distributed Energy Resources (DER) or small power plants could also be aggregated (e.g. in Virtual Power Plants (VPP)) to reduce the complexity of negotiations and contracts.

This general use case was developed taking into account the following detailed use cases:

- Revenue Optimization based on Price Profile of External Energy Suppliers
- Business Interaction based on Demand Response Optimization
- Business Interaction with DERs

4.2.1.2 Microgrid Operator sells Balancing and Ancillary Services

The cooperation for the electrical network stabilization and balancing is rewarded. Incomes are bigger for the same energy amount traded, so it would be interesting for the Microgrid Operator point of view to participate, if possible, in this market instead of the retail market. This could be possible for Microgrids where generation can be modulated by choice, e.g. fuel generators, biogas, geothermic, or water turbines.

4.2.1.3 Microgrid provides Islanding Mode

The Microgrid Operator provides a new service to the Overlay Grid Operator: The Microgrid with all its producers / consumers can switch to islanding mode whenever the Overlay Grid Operator requests this service. A reason for the Overlay Grid Operator to initiate the switch to islanding mode could be, for instance, an emergency case in the overlay network.

- **Control & Management Use Cases**

4.2.1.4 Balancing supply and demand on different time-scales

Reliable & efficient performance of a Microgrid is based on the central tasks of load balancing and power stabilization. DERs or small power plants could be aggregated (e.g. VPP) as well as the demand (consumers) to ease the burden of load balancing.

These use cases are comprised of the following details:

- Forecasting energy production and consumption on different time-scales
- Monitoring
- Data Management
- State analysis and sub-sequent actions
  - State analysis and sub-sequent actions for providing ancillary services
  - State analysis and sub-sequent actions for dispatching a contracted energy profile
  - State analysis and sub-sequent actions for providing operation in Islanding mode
- Optimal power flow (intelligent loss minimization)
- Switching to and from Islanding Operation

4.2.1.5 Demand-side management

Demand side management (DSM) is the process of managing the consumption of energy with to goal to increase the grid reliability and stability. Various controlling scenarios and functions take place in order to achieve energy consumption management. Monitoring energy consumption is a reusable and horizontal function which is necessary for other DSM scenarios. Intelligent Load Shedding, Automated Load Shifting and Price-based Shifting are alternative ways to control energy consumption on different times-scales.

These use cases are comprised of the following details:

- Continuous determination of available controlling power range on different time-scales
- Intelligent load shedding in critical operation
  - Automated Load Shaping
  - Price-based Load Shifting

4.2.1.6 Supply-side management

This section about supply-side management gathers all aspects related to monitoring and control of decentralized supply. Therefore, supply-side management describes the most relevant use cases which are somehow related to DER units. This contains use cases about monitoring the state of DER units as well as use cases about controlling the active and reactive power generation. Goals of these use case reach from secure operation of the Microgrid via optimized power quality within the MG until ancillary services offered to the overlay grid operator by control of DER units. Some of these use cases may be based on similar technical principles, but are pursuing different goals. Therefore, they will be listed separately in order to be able to separately examine the ICT requirements at a later stage.

This general use case was developed taking into account the following detailed use cases:

- Continuous determination of available controlling power range on different time-scales
- Control services
  - Active Power Voltage Control
  - Reactive Power Voltage Control
  - Reactive Power Compensation
  - Voltage Var Control
  - Enhance Local Power Quality
  - Primary reserve
  - Secondary reserve
  - Tertiary reserve

4.2.1.7 Black Start in Islanding mode

If a system disturbance provokes a general black out such that the Microgrid (MG) was not able to separate and continue in islanding mode, and if the system is unable to restore operation in a specified time, a first step in system recovery will be a local Black Start.

Two types of Black Start (BS) functions are needed:
- Local Black Start of the Microgrid after a general system black out;
- Grid reconnection during Black Start.

4.2.1.8 Auto-configuration

When new devices (e.g. DERs or intelligent appliances) or sub-systems (e.g. Home/Building Energy Management Systems) are installed in or at the edge of the Microgrid they automatically configure themselves (also frequently denoted as Plug and Play). The Microgrid operator can access the devices in a secure and trusted manner. Based on the ownership different access rights control the access of the Microgrid Operator to the device. The devices can describe their capabilities to the Microgrid operator and specify their services for monitoring and control.

This general use case was developed taking into account the following detailed use cases:

- Plug and Play of Smart Appliances in house
- Registration of devices owned by the Microgrid Operator at the Microgrid Control Centre
- Registration of DERs owned by the DER owner at the Microgrid Control Centre
- Registration of a Home/Building Energy Management System at the Microgrid Control Centre

4.2.1.9 Long-term Planning of Microgrid Infrastructure Design and Upgrading

The Microgrid Operator establishes a planning tool that accesses the data of a comprehensive Microgrid Data Base (MG-DB) – this DB may be the monitoring DB and contains all actual management and configuration data and details of all devices and entities inside the Microgrid. In case of new devices, customers, generators and status information the MG-DB is immediately updated.

In addition, a forecast service is taken into account (data of an F-DB) to respect future expectations for e.g. customers, generated power etc.

An offline simulation is started (planning tool) to check the proper operation of the whole Microgrid in case of integration of the new entities. In case of a negative result of the simulation (expectation of problems in the Microgrid) suitable countermeasures are to be found and tested with the simulation tool. For the planning of the future infrastructure, updated data of future consumption and regulation changes are to be taken into account.

4.2.2 Summary of WP3 ICT Requirements before Consolidation

WP3 ID	Name	Category	Short Description	Priorities
1	Scalability	Scalability	Scalability is the guarantee that a system can grow without compromising its operations. The Microgrid Control Centre cannot be collapsed if its success leads him to grow even more than originally expected.	COULD
2	Conformance to standards	Interoperability	Monitoring and control are two basic functionalities of the Microgrid Control Centre. The Microgrid Control Centre communicates with a large set of different devices from different domains (e.g. from intelligent loads to large wind turbines). To ensure interoperability the communication should rely on well-known and frequently used standards like IEC 61850, IEC 61968/61970 (CIM), or IEC 60870-5-101/104 (Telecontrol) and others. Also to be respected are specialized communication standards like - IEC 61400-25-4 for wind turbines,- IEC 62270 Hydroelectric power plant automation - Guide for computer-based control, - IEC 62271 Standards for high-voltage switchgear and control gear,- IEC 62325 Standards related to energy market models & communications, IEC 62351 Power System Control and Associated Communications - Data and Communication Security, and others	COULD
3	MG Controller and management system applicability	Interoperability	MG Controller and management system should be applicable for wide range of Microgrids. Controller and management system with generic configuration will support several types of Microgrid setups.	COULD
4	Mappings between different information models	Interoperability	Monitoring and control are two basic functionalities of the Microgrid Control Centre. The Microgrid Control Centre communicates with a large set of different devices from different domains (e.g. from intelligent loads to large wind turbines). Today a large number of different standards exist and it is very likely that this will also be true in the future. To ensure interoperability between different standards with different information models the standards have to be harmonized. A flexible mapping tool is needed to map monitoring and control data points from different information models onto each other. E.g. the mapping tool should be designed to minimize the manual input and mapping information should be re-usable. An important mapping guideline, for instance, is IEC 61850-80-1 which describes a mapping from IEC 61850 data to IEC 60870-5-101/104. Mapping to IEC 60870-5-101/104 is and will stay a very important task since a large number of legacy devices and systems are only able to run this standard, and switching to other control systems is a big challenge for each system operator which will not be realized very soon.	COULD

5	Data bus	Data management	Data management is one of the key features of the Microgrid Control Centre (MGCC) where high volumes of real-time and historical, static and dynamic operational data are distributed and/or replicated for parallel processing and access. That means up to thousands of data points have to be instantaneously processed, coordinated, manipulated and interpreted if the Microgrid Operator wants to take full advantage of all resources. Following a service oriented architecture the Microgrid Control Centre should include a data bus which enables the communication and information exchange between different services in the MGCC. The data bus should provide different communication services (e.g. request/response, publish/subscribe, transactions). Furthermore, it should support different levels of Quality of Service because different applications have different demands, e.g. with regard to latency, frequency of data exchange, quality or time synchronization.	COULD
6	Database system	Data management	Data management including a database system is one of the key features of the Microgrid Control Centre (MGCC) where high volumes of real-time and historical, static and dynamic operational data are distributed and/or replicated for parallel processing and access.	COULD
7	Self-organization	Automation	If a system disturbance provokes a general black out such that the Microgrid (MG) was not able to separate and continue in islanding mode, and if the system is unable to restore operation in a specified time, a first step in system recovery will be a local black start. The different components of the MG have to auto-organize themselves before reconnecting to the grid	MUST
8	Coordination	Automation	If a system disturbance provokes a general black out such that the Microgrid (MG) was not able to separate and continue in islanding mode, and if the system is unable to restore operation in a specified time, a first step in system recovery will be a local black start. The local controllers of the MG need to dynamically coordinate each other and with the MG control centre for the recovery	MUST
9	Distributed Processing	Processing	For balancing supply and demand the Microgrid Control Centre has to run the state analysis and define the sub-sequent actions. These tasks include power flow calculations and forecasting models. To minimize processing latency the jobs could be processed in parallel and distributed across different machines. Also for forecasting, planning and revenue in the revenue distributed processing capabilities are crucial.	COULD
10	High Demand for Computing Resources / Processing	Processing	For some use cases, it is necessary to provide high performance computing resources for calculation and simulation models in the Microgrid Control Centre including real-time processing. One example is switching to islanding mode in order to quickly check availability of electrical resources in case islanding of the Microgrid is required. Also for long-term planning it may be necessary to provide high performance processing for large-scale planning and simulation. In order to optimize power flow in case of switching to islanding mode, high demand for computing resources for calculation and simulation models in Microgrid Control Centre is required. In order to optimize power flow in case of switching to connected mode, medium processing demand for adaptation to electrical parameters in Overlay Grid is required.	COULD

11	Demand management based on criticality of loads	Processing	MG management and control system shall control loads and enable smart load controlling (cancellation of loads, shifting if loads etc.).	COULD
12	Network Configuration	Auto-configuration	When new devices (e.g. DER, Network Smart Devices) or sub-systems (e.g. Home/Building Energy Management Systems) are installed in or at the edge of the Microgrid they automatically configure itself (also frequently denoted as Plug&Play). This requirement focuses on IP address configuration and addressability of the device by the Microgrid Control Centre.	MUST
13	Device Description	Auto-configuration	When new devices (e.g. DER, Network Smart Devices) or sub-systems (e.g. Home/Building Energy Management Systems) are installed in or at the edge of the Microgrid they automatically configure itself (also frequently denoted as Plug&Play). This requirement focuses on the description of the capabilities of a device or sub-system	MUST
14	Registration & Look-up	Auto-configuration	When new devices (e.g. DER, Network Smart Devices) or sub-systems (e.g. Home/Building Energy Management Systems) are installed in or at the edge of the Microgrid they automatically configure itself (also frequently denoted as Plug&Play). This requirement focuses on the registration of the device or sub-system at a registry which is operated e.g. as part of the Microgrid Control Centre.	MUST
15	Reliability and Availability (R&A) for the systems	Reliability and Availability (R&A)	For all use cases, the reliability and availability of all devices and systems are crucial; this is especially true for the control centre systems. All possible actions and monitoring concepts must be installed to avoid any breakdowns of the systems. The acceptable breakdown/unavailability times may be different for the different systems and may be defined accordingly. It is also required to install fallback or replacement systems that can almost immediately take over crucial actions and processes. If availability and reliability cannot be guaranteed for all the devices the overall system has to be robust with regard to disturbances and failures to ensure the stable operation of the Microgrid.	MUST
16	Reliability and Availability (R&A) for the communications	Reliability and Availability (R&A)	For all use cases, the reliability and availability of the communication between the different devices / systems is also crucial; failure in communication (especially concerning control messages) may harm the electrical network to a very deep extent. Failures in electrical devices also must be reported and recognized immediately. Resilience strategies must be planned and ready for taking over communication whenever there is a bottleneck in communications. Strategies and algorithms must be prepared to recognize problems and bottlenecks in communication in time (i.e. before they happen).	MUST
17	Modularity of Hardware Devices	Future Proofness	Communication technology is developing rather rapidly. More and more bandwidth will be provided for communication. Wireless reliable secure communication will replace wired communication more and more in the future. It should be easy to replace one communication technology with another one simply by exchanging HW modules at the network devices. Changing or upgrading the physical medium should have no impact on other layers, especially the application layer.	Optional

18	Modularity of Software Devices	Future proofness	IT technology is developing rather rapidly. More and more flexible communication and service architectures will be provided. Wireless reliable secure communication will replace wired communication increasingly in the future and Plug&Play will dominate modular designs. It should be easy to replace or extend communication or application service modules by exchanging or adding SW modules. Changing, adding or upgrading services should not cause redesigns.	Optional
19	Publish / Subscribe	Communication Services	In asynchronous messaging a system places a message in a message queue based on internal logic or event and does not need to wait for a reply to continue processing. Subscribers express interest in one or more message classes, and only receive messages that are of interest for them. .	COULD
20	Request / Response	Communication Services	Data will be sent on a request, when a system is asking for certain information and the Data Provider response back to that system with requested information or at least acknowledging the request.	COULD
21	Time synchronization	Communication services	To achieve network wide synchronization of control tasks on different time-ranges and scalability up to hundreds of systems, while being robust to topology changes and failures, a time-based synchronization method by utilizing concepts of e.g. time-stamping and skew compensation with linear regression is needed.	COULD
22	Latency	Quality of Communication Services (QoS)	Latency is either one-way delay or round-trip delay. It is always very important to additionally define at which communication layer a latency value should be measured (bit level, TCP packet level, application layer). Values for latencies or delays must reflect the transmission and propagation times that are acceptable for the communication between devices / systems so that information is available in time and possible reactions can be initiated or handled as necessary. The main distinction for latency is: - RT (real-time): delay is deterministic and generally in the range of milliseconds - non-RT: delay is in the range of seconds or more	MUST
23	Bandwidth – Throughput / Goodput	Quality of Communication Services (QoS)	Bandwidth is a measurement of maximal possible number of bits or bytes that can be transferred over a communication link (wired or wireless) within 1 sec. respecting all channels served at the same time. Throughput is the real number of bits and bytes that can be transmitted between 2 endpoints of communication within 1 sec., dependent of the number of other communication channels on the same line or medium, the communication environment etc. Goodput is the number of packets, bits or bytes that are correctly transmitted to the receiving data endpoint within 1 sec. It is mostly lower than the throughput because retransmission of information may be necessary in bad or disturbed connections.	COULD
24	Packet Loss	Quality of Communication Services (QoS)	Packet loss here means the maximum acceptable percentage of lost packets on a communication link. The lost packets may be retransmitted (reducing the goodput) or not. In the latter case the acceptable packet loss rate means the number of lost packets that would allow the receiving endpoint to realize the communication with a quality that may still be acceptable for the user (i.e. in video transmission:	MUST

			with which percentage of lost packets a video transmission may still be reasonable for the user at the receiving end?)	
25	Priority	Quality of Communication Services (QoS)	Priority in transmission scheduling is an easy way to prefer data of one connection compared to other connections.	MUST
26	Remote control of equipment	Management	The Microgrid Operator needs to remotely control the power electronics of the DER Units in order to provide system services to the overlay grid or to control technical parameters within the Microgrid.	COULD
27	Asset management	Management	Inventory of equipment's, appliances, lines in the Microgrid.	COULD
28	Topology view	User Interface	Visual view of generation and consumption locations (preferable connection with asset management).	COULD
29	Security Services	IT Security	Security is a very important requirement for the future. To which extent WP3 will handle this topic must still be discussed.	MUST

Table 2: WP3 ICT Requirements Summary

4.3 WP4 – Smart Buildings

This Work Package aims to define the scope of the smart buildings domain, analyzing different buildings typologies (smart homes, residential buildings, office buildings, data centres and hotels, also called scenarios in the context of this document) as holistic systems that encompass all the physical components of the building. For this analysis use cases were defined which deal with energy-related functions of the building which need the support of ICT systems. Use cases across the different scenarios defined share a set of common external actors, namely external and internal environment, organizations such as energy service companies or facility staff, and external entities such as electric utilities or the micro grid where the building might be inserted; while other actors are specific for each scenario.

4.3.1 WP4 Use Cases Summary

1. Home Domain Use Cases

4.3.1.1 Display the global energy consumption and costs using data from Smart Meter and Metering Operator

The customer is presented with information about the global energy consumption of his/her house. The Smart Meter provides a sub-set of its data, included instant power. Data are dispatched either periodically, or upon request and in case of transition (for example for tariff period change). The Smart Meter provides its data to the HAN either directly, using its own interface, or through a meter service module.

4.3.1.2 Display the global and per appliance energy consumption and costs, either realized and/or forecasted.

In this Use Case, added to the previous Use Case #1 (Section 3.6.1.1), the customer is also informed on the energy consumptions of the single appliances. The Smart Meter and meter service module functionality is the same as in Use Case #1. In addition, they also provide near real time instant power information to allow Smart Appliances to calibrate their energy consumptions with respect to the subscribed limited power.

The Home Gateway functionality is extended from Use Case #1. It provides to user appliances a single point of contact to publish their respective energy consumption and power information.

Each appliance: either directly, in case of a smart appliance, or through a smart plug, displays its own energy consumption/power drawn data, dispatches its own energy consumption data over HAN, receives over HAN the total house energy consumption and displays the total house energy consumption.

4.3.1.3 Warn the consumer if the available total power (in the home) is not sufficient to run a Smart Appliance

The Smart Appliance estimates the maximum power that will be consumed during its next operation (ex: cycle). If there is a risk to exceed the threshold of the contracted subscribed power, a warning is emitted and displayed on the appliance or other customer interface(s).

4.3.1.4 Direct load control

The interruption of certain uses becomes a virtual means to solve peak loads on the grid. Each provider may contract with a number of his customers to agree to have some of his appliances interrupted a few hours per year. In exchange, the customer is rewarded for giving this facility. The direct load is triggered by the provider with notice of the customer.

4.3.1.5 Dynamic pricing of electricity

To move out peak loads, provider proposes a tariff of electricity higher during certain periods of the day or during certain days in order to invite his customers to delete or shift various uses or lower their consumption in its housing during these periods. The regular daily and weekly price variation is known by the customer. For a small number of peak days, a special peak day tariff may apply, which is particularly high; the customer is informed before every peak day.

These tariffs are made in order to encourage the customer to lower his consumption during the most expensive periods; they may be handled either directly if the appliances are smart enough, or through a control appliances module which controls the equipment.

4.3.1.6 Emergency Load reduction

After the failure of the network or of a mean of production, the users are relieved, without notice, to avoid a blackout. The use of these load reductions should be very marginal (less than 10 hours per year). The distributor controls these emergency load reductions.

4.3.1.7 Handle dynamic power cap

Direct load control could be done in an alternative way than the one presented in Use Case #4 (Section 3.6.1.4). instead of directly sending reduction orders to the appliance control module, the supplier would send to the meter or to the breaker a lower value of the maximum power for the home (or the power cap), that lasts for a short period (typically a few hours). The customer is notified when this reduction occurs and handles this reduction of the power cap with his smart appliances and/or through the appliance control module which controls the equipment and optimizes their operation under given power and energy cost conditions, as in the Use Case #5 (Section 3.6.1.5). Unless the consumer derogates, some appliances may have to be stopped and the start of others may be forbidden or delayed, in order to stay under the low value of the global power cap.

4.3.1.8 Optimize energy in a home equipped with smart appliances and smart generation and storage

This use case describes an “extreme” use case where the demand may be shaped in many ways, and has been inspired by the Beywatch project (http://www.beywatch.eu/). The home is supposed to be equipped with:

- Many smart appliances that are today under development : HVAC system, either for winter or summer, hot water tank, smart white goods (washing machine, dishwasher, dryer, fridge/freezer, …).
- Electrical vehicle, which may either consume energy for its needs but also store and make available a share of the stored energy in case of emergency needs on the grid.
- Thermal renewable sources, as solar thermal panel which may provide hot water for the domestic use but also for the washing machines.
- Electric renewable generation, as photovoltaic panels or wind turbines.
- Energy storage means, either in thermal form through the different appliances (as hot water tank for heat storage, or fridge freezer for cold storage), or in battery.

Residential Buildings Use Cases

4.3.1.9 Display Energy Consumption

This use case allows an actor to display or produce reports of the current as well as of the historical energy consumption at the building level (excluding energy used in the apartments). It includes both electricity and gas (cumulatively or separately). The use case is understood to allow plots, graphs and extracts (for data-interchange purposes) to be easily obtained through a web-based GUI. This use case obviously relies on the "Monitor Energy Use" use case and "simply" adds the ability to visualize and extract detailed information / data from the database.

4.3.1.10 Provide Emergency Lighting

This use case uses the power stored at the building level or the power generated by building-level photo-voltaic panels or wind turbines to provide emergency lighting in the common areas or, also, private apartments, if so configured, in the event of a grid power failure.

4.3.1.11 Provide Graceful Elevator Shutdown

The idea behind this use case is to allow the system to employ the power stored at the building level to provide emergency electricity in the elevator shafts, when and where necessary, in the event of a grid power failure. The focus here is mostly elevators and, in particular, elevators that were currently in motion or / and had passengers in when the power failure occurred.

4.3.1.12 Store Electricity Locally

This is another "physical" use case that represents the capacity of the building to store electricity locally and the availability of an ICT infrastructure to allow monitoring and historical / real-time reporting of:

- how these locally stored energy reserves are built (i.e. which are the sources contributing to the electricity store - locally harvested energy or grid) and,
- how they are depleted (e.g. which are the loads that draw from this electricity store).

4.3.1.13 Store Hot Water Locally

This is another "physical" use case that represents the capacity of the building to heat or store hot water locally in anticipation of future needs or for reasons of economies of scale. Since this is a central component for the whole building, economies of scale can presumably allow use of better quality materials and more expensive or bulky insulation methods that would be possible had the water tanks been distributed in every apartment.

4.3.1.14 Centrally Heat Water for Private Uses

This use case allows the system to provide hot water 24/7 (or for other extended time periods less than 24/7) for all building residents while at the same time maintain a metering capacity capable of allocating costs to specific apartments. Certain buildings, for reasons of economies of scale, include infrastructure to centrally heat hot water and make it available to residents. This infrastructure can include PV panels, solar panels, highly efficient water heaters, or highly insulated hot water tanks. Reasons for doing so at a central building level can include economies of scale, reduced maintenance requirements or even civil engineering considerations. However access to a communal resource encourages waste so the idea here is to combine the central infrastructure with metering appliances that can measure the hot water consumption of each household. In this way all residents gain from the economies of scale and the reduced maintenance while at the same time being charged only in relation to their actual usage.

4.3.1.15 Provide Communal Hot Water

This use case foresees the installation of solar panels and use of thermal energy to heat water in a shared tank for use in common resources (e.g. swimming pool). This use case is adapted from the Best Energy project no. 238889 ICT-PSP, Built Environments Sustainability and Technology in Energy / Deliverable D1.1 / pilot B1 (Paco Yoldi Sports Centre) and synthesized with ideas coming from BeyWatch project (www.beywatch.eu).

4.3.1.16 Optimize Lighting

This use cases features a smart lighting system to conserve electricity and reduce costs in the lighting of common areas in the building. The system is ICT-based and fully automated and is used for controlling

lights in all common areas of the building. The system makes use of motion detection sensors, an astronomical clock (sunrise and sunset) and dimmable lights. This system is considered an agent of the "Energy Manager" actor who is responsible for configuring high-level business rules on which the system acts.

4.3.1.17 Optimize Indoor Climate Control

This use case represents a functionality that comprises sensors that monitor heat, CO2 levels and humidity in the common areas together with an outside weather station and an intelligent control system to ensure that the building adjusts to the configured setting for a comfortable indoors environment. The intelligent control system is considered an agent of the "Energy Manager" actor. PV panels or the building's energy storage reserves provide the energy required for powering the actuators that open the windows to optimize the flow of fresh air when the outside conditions are right.

2. Office / Public Building Use Cases

4.3.1.18 Check energy use

The Building Energy Management Systems (BEMS) provides regularly updated historic, real-time and/or forecast energy usage data of the office building via displays/information screens/web browsers to the end-users with the goal to motivate the staff to use energy conservatively. The BEMS also provides weather forecast and predictions of indoor environment conditions.

4.3.1.19 Check acute alerts

Information about the energy use of the office building is available remotely. If an anomaly situation is detected, an alert will be sent.

4.3.1.20 Allow Real-time DR events in the service centre

Real-time Demand Response (DR) events are received by the energy manager in the building. The energy manager could decide the better strategies to take advantage of these events.

4.3.1.21 Check DR period in the office room

The rationale of this use case is that the BEMS should provide to the end users (office workers) through the user interfaces available in the office rooms information about the Demand Response (DR) actions that have been taken. Means should be granted to end users to override these actions, especially in shared spaces such as meeting rooms. Information about DR actions is always accompanied with advices to the end-users for using energy conservatively.

4.3.1.22 Energy coaching

This use case consists on a bidirectional exchange of information between the end users and the Building Energy Management System. On one hand the BEMS provides the end users with information about the amount of energy consumption and costs associated to each energy hungry device they normally use, on the other hand the BEMS learns from the ordinary behaviour of the end-users in order to adapt the operation of the devices. A concrete example of this is to switch the office room status to a standby condition (for lighting, and maybe HVAC) when the user leaves the office.

4.3.1.23 Check benchmarking in districts

The energy consumption data from buildings in the district is obtained and provided to the end-user to enable benchmarking.

3. Data Centre Use Cases

4.3.1.24 Optimize the data centre air conditioning

The air conditioning systems (with their heat pump for winter) comes to represent 50% of the consumption of a data centre. A real-time monitoring of temperatures (which vary with the load of servers) allows significant savings in energy consumption.

4.3.1.25 Optimize the free-cooling in the data centres

Free cooling is an economical method of using low external air temperatures to assist in chilling water, which can then be used for industrial processes, or air conditioning systems in green data centres. The free-cooling systems are so much less expensive compared to air conditioners in terms of power consumption. However, unlike air conditioners, their efficiency must take into account the humidity factor. A real-time monitoring of humidity allows to the system to operate with adequate ventilation. HVAC (Heating, Ventilation, and Air Conditioning) refers to technology of indoor data-centre environmental comfort. HVAC system design is a major sub-discipline of mechanical engineering, based on the principles of thermodynamics, fluid mechanics, and heat transfer. In HVAC in winter months, large commercial buildings' interior spaces may need cooling, even while perimeter spaces may need heating. Free cooling is the production of chilled water without the use of a chillier, and can be used generally in the late fall, winter and early spring, in the Northern Hemisphere.

4.3.1.26 Optimize server power usage

The collection of real-time power consumption data constitutes an essential capability for power monitoring. Without this data, the best approximation for server power usage comes from the manufacturer's specifications. To use the nameplate numbers as a guidepost requires the allowance of a hefty safety margin. To honour the safety margin in turn leads to data centre power over-provisioning and stranded power that needs to be allocated in case it is needed, but is very unlikely to be used.

This situation results in over-provisioned data centre power, overcooling of IT equipment, and increased total cost of ownership (TCO). The steps described in this use case act as a "load balancer", in order to determine how many additional servers having similar power cap settings can be added to the rack without overshooting the power quota allocated.

4.3.1.27 Manages business continuity

When unforeseen circumstances like power outage and cooling system failure occur, a service continuity optimization is made possible through an Intelligent Power Node Manager SW and an Energy Management SW that force the servers to a lower power consumption and to a low heat generation. In these scenarios it may be appropriate to set aggressively lower power caps though performance would be affected. Please note all servers may not meet the aggressive power limit that is set. It depends on the application that is running and if the minimum power limit that can be honoured which depends on the operating system and the application load at that point. The use case illustrates how it works at a data centre location or a group of servers.

4.3.1.28 Optimizes power workload maintaining a high quality of services (QoS)

Workload profiles are built and a maximum performance loss target set. Experiments determine how much capping can be applied before the performance target is hit. The approach is to match actual performance against service level requirements. In this way, using an Energy Management SW, for workloads that were not processor intensive, it's possible to optimize server power consumption by approximately 20 percent without an impact on performance. For workloads that were processor intensive, typically, for a 10 percent power reduction, performance decreased by 14 percent. In this way the data centre financial manager can offer at the business client the best service quality at the lowest price and at the lowest power consumption.

4.3.1.29 Choose between multiple service classes in function of the workloads priority

Consider two service classes for workloads, namely: high and medium priority workloads. The high priority workloads run on unconstrained servers; they can take all the power they need to run as fast as they can. Medium priority workloads are assigned to power capped servers. These will run more slowly, but they will still run. The financial manager presents at the customer a tariff that depends from the expected level of the quality of services (QoS). Typically, this approach not only allows saving money for the end user but it can also allow saving energy in the data centre up to 25 percent.

4. Hotel Use Cases

4.3.1.30 Execute strategy

The strategy includes energy consumption and generation. In collaboration with the utility a hotel can participate at the energy exchange and offer positive and negative reserve energy. A strategy includes a tolerance range in temperature (swimming pool, room) which has an effect on the possible energy reserve that can be offered. In addition to that energy storage can be installed in order to optimize against a set of KPIs defined by Hotel Management.

4.3.1.31 Define Energy KPIs

The Hotel Management defines certain key performance indicators (KPIs), which characterize the performance of the hotel building automation system with regard to energy.

4.3.1.32 Monitor KPIs

The system provides predefined KPIs like energy consumption, cost, etc. to the Hotel Management.

4.3.1.33 Set Prices

Depending on the current production and load situation on the grid or an extrapolation of the current situation the utility can change the price of different forms of energy.

4.3.1.34 Request load switch

An actor, typically a guest, requests to switch a load on or off. The request influences the total load of the system, which then has to be stabilized according to the rules implemented by the Energy Manager and the KPIs defined by Hotel Management.

4.3.1.35 Shed load

The energy manager decides to disconnect certain loads from the network, according to the strategy defined.

4.3.1.36 Generate energy locally

In order to cope with spikes in demand or drops in supply, the Energy Manager decides to generate some energy locally. Especially for renewable energy sources the decision to generate energy locally may also be triggered by external factors such as wind speed, intensity of sunlight, etc.

4.3.1.37 Store Energy

Based on the current load/price situation and a prediction, energy from the grid is stored locally for future use.

4.3.1.38 Request energy from the net

The energy manager requests energy from network.

4.3.2 Summary of WP4 ICT Requirements before Consolidation

WP4 ID	Name	Category	Short Description	Priorities
1	ARQ/FEC	Data Communication	The data link layer must provide sufficient error detection and/or error correction to enable effective communication. In case of error detection, an ARQ scheme or a implicit failure notice to the user must be implemented	MUST
2	Bandwidth of building access network	Data Communication	The connection needs to guarantee the necessary bandwidth so as to send information on the building (identifier), and power and energy information for each one of the appliances that are being monitored and managed. The required bandwidth must be suitable for fixed and mobile communications between the platform and the	MUST

			building gateway.	
3	Connectivity : always on	Data Communication	There must be an always on connectivity between the service platform and the home gateway, either fixed or mobile. Connectivity between the building gateway equipment and the platform must be 'always on' in the sense that at any time the consumer wants to access the service (through the corresponding applications, no matter the platform), connectivity with the building must be established, to get up to date information on power and energy consumption and to send control commands if requested by the consumer. This requirement could be modulated according to criticism of considered EE services.	MUST
4	Connectivity : high-level	Data Communication	This requirement relates to the need to “connect” in all relevant senses of the word all devices, appliances, and more generally all physical entities that need to have a network presence inside the extended perimeter of the building management system. Getting this presence means getting connected at all relevant levels, from physical to application level, even in the absence of some of the intervening network protocols. This connectivity includes being part of a relevant device/appliance entity ontology, which corresponds to the highest level of connectivity, i.e. the semantic level.	MUST
5	Latency	Data Communication	Latency requirements are not critical within the building and can easily be met by all current networking technologies; specific latency requirements arise in the case of separation of the BEMS between a local and a remote part;	COULD
6	Physical layers	Data Communication	The physical layers used must allow the coexistence of several communication standards by separation in the frequency, time, coding or spatial domain according to standards	MUST
7	Control commands latency	Data Communications	Control commands from local/remote user interfaces must reach physical appliances with minimum delay (acceptable by the human user). When the consumer connects to the energy efficiency services, either locally or using a remote interface (any application, independently from the platform used: pc, mobile, Smartphone, etc.), control commands must be applied in the physical appliance in a time perceived by the consumer as acceptable (bellow 2 seconds)	MUST
8	Energy Services and applications decoupled from available in-home/building communications technologies	Data Communications	Energy services and applications, while enabled through in home/buildings communications, must not depend on one or some specific communication technologies and remain as communication technology agnostic" as possible.	MUST
9	Local processing and storage	Data Processing and Storage	Data processing and storage requirements are indispensable for any sort of building-level intelligence and so as to back and inform any communications of building-level software with consumers (through a human-machine interface) or with the grid (through an interoperability interface). See more extended discussion in referenced document.	SHOULD

10	Remote processing accumulative values	Data Processing and Storage	The platform must offer a way for calculating average consumptions and energy related data and costs: per day, week, month, and year.	MUST
11	Remote processing and storage	Data Processing and Storage	The consideration of demand-shaping measures and the implementation of peak shaving capabilities require the grid administrator to have some sort of visibility into the contracts the various loads subscribe to. This is to allow the grid administrator to use a system of compulsory or incentives-oriented measures so as to bring about the intended changes in the load curve. As such, it is necessary to maintain information about the contract model of each subscriber, the options available to that model, and the extent to which some of these options have already been used. Moreover to correctly anticipate future needs both current, real-time, energy demands as well as historical information should be available, on which to base reliable forecasts and ensure the timely initiation of load-shifting measures. Furthermore, and subject to privacy requirements, socio-economic profiles may also need to be available for the various subscribers (even some rough categorization).	MUST
12	Remote processing of comparative values	Data Processing and Storage	The platform should be able to calculate average consumptions and energy related data and costs for buildings with the same profile (homes, depending on the size and use; home buildings; data centres; hotels; SMEs, etc). Average consumptions and costs per day, week, month and year	SHOULD
13	APIs for ESCOs	Interoperability	The platform (FI-WARE) should offer a standard API for ESCOs so that monitoring and control capabilities available in a building are published for the development of a service. This capabilities need to be qualified with the list of end user roles that can make use of such functionality. For instance, monitoring is not so critical, almost everybody could access these data (taking privacy into account) but control options should be offered only to managers in homes buildings or SMEs.	SHOULD
14	Common data models (CDM)	Interoperability	Definition of common data models (CDM) per type of sensor/appliance. In order to perform energy optimization on behalf of the consumer, home appliances must be modelled in a common way so that the intelligence in the system is able to monitor them, know control capabilities, programming capabilities and have at any moment information on the reachability of the device.	MUST
15	External Interoperability	Interoperability	For the purposes of peak shaving, and demand-side management the residential building, on the one hand, and the smart grid, on the other, need to engage in a conversation that's rich in semantic content and could be very heterogeneous in the mechanics and modalities it employs. The object of this "conversation", which can be described as a "protocol" (understood here in a broad sense) is to convey pertinent information and measurements so as to both: (a) enable the grid to communicate to the building a set of rules / imperatives or incentives / counter-incentives, related to demand-side management and, on the other hand to: (b) allow the building to report information, measurements and projections to the grid. See more extended discussion in referenced	MUST

			document.	
16	Identification of devices	Interoperability	The network must allow for unique identification of every device on the network regardless of the physical network it is connected by	MUST
17	Internal Interoperability with existing building systems	Interoperability	Communication layer shall enable interoperation of building management system and other systems existing in the building: access controls, surveillance systems, fire alarm systems.	MUST
18	Join networks	Interoperability	The network layer must allow for the combination of two or more separate physical networks into one logical network	MUST
19	Profiles	Interoperability	Interoperation with building management systems should allow for definition of personal profiles with different sets of privileges. Concurrent access to data of the different profiles shall be granted	SHOULD
20	Split networks	Interoperability	The network layer must allow for the possibility to logically split an existing network into several subnet works	MUST
21	Standardization of sensor/appliance monitoring and/or control capabilities	Interoperability	The devices that are published so that they are available from outside the home should provide a common API (depending on the type) to publish the basic common monitoring and/or control capabilities they offer for service providers. Mechanism should also exist for extended capabilities that some devices could offer beyond these common ones.	SHOULD
22	Standardization of sensor/appliance evening capabilities	Interoperability	The FI platform should provide the means for home sensors/appliances to send events (triggered by the sensor/appliance itself)	SHOULD
23	Standardization of sensor/appliance programming capabilities	Interoperability	The devices that are published so that they are available from outside the home should provide a common API (depending on the type) to publish the programming capabilities they offer for service providers	SHOULD
24	Standardization of sensor/appliance publication protocol	Interoperability	There should be provided a mechanism for publishing the sensors that can be remotely monitored in the home. This would enable the use of these sensors by other services different from home energy efficiency services that can manage the information provided in a local manner.	SHOULD
25	Unique building identifier	Interoperability	Each building must have a unique identifier: its geographical location can be used for this if non ambiguous (same building split and under responsibility of several parties) and standard for representation of this location has been agreed on with external parties beforehand	MUST

26	Remote alarm management	Interoperability	User interface shall enable remote alarm visualization and management by multiple operators of the following subsystems: access controls, alarms from thermal/electrical systems, system maintenance alerts, fire detection. All subsystems should be accessible from the same user interface	MUST
27	Enough data storage capacity	Processing and Storage	Requirement will be met without problem, unless old dat is never discarded	MUST
28	Check Energy Use	Reliability & Availability	Availability of access to data of current status of the building shall be guaranteed both locally and remotely from Internet connected devices 95% of time	MUST
29	Fall back mode	Reliability & Availability	The system should be able to identify a loss of the communication systems and be able to switch to a fallback mode	SHOULD
30	Reliability for residential buildings	Reliability and Availability	Reliability of the various ICT subsystems deployed at a residential building (these subsystems being used to deliver the various energy efficiency use cases) is critical. The requirement for reliability obviously comprehends not just the hardware but also the software components and not just each one of them separately but also taken together (e.g. reliable coordination and protocols in a distributed setting). However, failures are not life threatening since we are concerned with the reliability of the ICT superstructure and not with the reliability of the underlying energy infrastructure. To that end, architecture should be designed to ensure that latter can survive a breakdown of the former. See more extended discussion in referenced document.	SHOULD
31	Air conditioning real time control system	Reliability and Availability	A real-time monitoring and control of temperatures (which vary with the load of servers) is required to allow significant reliability and availability of the data-centre functionalities.	MUST
32	Free cooling real time control system	Reliability and Availability	The use of free cooling system is required to ensure energy saving, reliability and availability at the data-centre in case the failures of its air conditioners system	MUST
33	Power meter usage	Reliability and Availability	This ICT requirement allows knowing the difference between the nominal (typically higher) and the one real of the power consumption of the servers in the data-centre. So, it is possible increase their number (offering more reliability and availability) without overshooting the power quota allocated.	SHOULD
34	Access based security	Security	The security concept may use access restriction (based on roles) together with physical location of input devices to implement the role based restrictions of users	SHOULD
35	Building Benchmarking	Security	Exchange of data among different office/public buildings shall be implemented in order to enable benchmarking at district or higher levels of buildings of similar characteristics. Data exchange is done in a network external to the buildings, and information provided to each building must not contain sensitive data, e.g. it should be decoupled from the identity of the building.	SHOULD
36	Data Encryption	Security	Solutions specification shall support data encryption of packets flow with the building systems	SHOULD

37	Disaster recovery system	Security	During primary AC power outage scenarios (due to fortuitous events or to intentional attacks); aggressive power capping can be applied to servers to reduce power consumption. This reduces the power drain on the Uninterrupted Power Supplies (UPSs) increasing the duration the servers can remain operational before on-site generators restore power and cooling.	SHOULD
38	Role based security	Security	The security concept must allow for a role based restriction of available actions of users	MUST
39	Security for residential buildings	Security	Use cases discussed in the residential buildings scenarios require the building to store or process information that while not sensitive (e.g. not health or credit-card related), is still personal and access to which by unauthorized parties would be construed as a privacy infringement. See more extended discussion in referenced document.	SHOULD
40	Security for residential buildings	Security	Use cases discussed in the residential buildings scenarios require the building to store or process information that while not sensitive (e.g. not health or credit-card related), is still personal and access to which by unauthorized parties would be construed as a privacy infringement. See more extended discussion in referenced document.	SHOULD
41	Workload profiler	Security	Develops and executes a series of experiments to characterize how much energy capping can be applied to the servers before the performance target is hit. If implemented, this requirement may increase the autonomy of the UPSs in case of blackouts due to fortuitous events or to physical intentional attacks.	COULD
42	Multiple service classes manager	Security / QoS	The high priority workloads run on high security servers; they can take all the power they need to run as fast as they can. Medium priority workloads are assigned to power capped servers. These will run more slowly, but they will still run. The financial manager presents at the customer a tariff that depends from the expected level of the security and quality of services (QoS).	SHOULD
43	Direct or emergency load control installation	Self-configuration	automatic and secure pairing of control appliances module with the IS of the provider, on one hand, and with smart appliances of the home of another hand	SHOULD
44	Display installation & configuration	Self-configuration	automatic and secure pairing of display with meter or meter module, on one hand, and with smart appliances of the home of another hand	MUST
45	Display installation & configuration	Self-configuration	automatic and secure pairing of display with meter or meter module, on one hand, and with smart appliances of the home of another hand	MUST
46	easy addition of new server in the energy monitoring tools of the data centre	Self-configuration	It should be easy and require no complex configuration to add a new server to the Intelligent Power Node Manager SW and an Energy Management SW of the Data Centre	COULD
47	easy addition of new wireless sensor to AC control system, of new component to the energy mgt/monitoring system	Self-configuration	It should be easy and require no complex configuration to add a new temperature sensor to the sensor network controlling the Air Conditioning of the Data Centre. Can be extended to other sensor types for HVAC system, other component of the energy management system	COULD

48	Energy Management & Optimization System Installation	Self-configuration	Automatic and secure pairing of control appliances module with the meter or the meter module on one hand, and with smart appliances of the home of another hand.	SHOULD
49	Meter module installation & configuration	Self-configuration	automatic and secure pairing of meter module with meter	MUST
50	Meter module installation & configuration	Self-configuration	automatic and secure pairing of meter module with meter	MUST
51	secure and easy connection of office workers to BEMS	Self-configuration	The office worker should be able to see the DR actions related to him and to its location without complex localization questions. If the worker is given the ability to derogate, this again should be left only to allowed people, based for example on their identity or location, without complex configuration but with enough security to prevent someone to "play" with these facilities.	SHOULD
52	secure connection of BEMS with DR Operator	Self-configuration	The DR events or dynamic prices must be certified by the originator before being taken into account, so that faked events (or price information) may be dismissed. The verification by the BEMS should require no difficult configuration yet be secure.	MUST
53	Self-Configuration general for networked devices	Self-configuration	Devices installed by the end consumer without any installer should be plug&play. However shouldn't allow unauthorized access from neighbours, hackers … nor allow the user to hack the neighbours. In installer is mandatory, his skills may not be in ICT but rather in electricity, energy management, etc.	COULD
54	Sensors, appliances etc. additional installation and consideration by the BEMS	Self-configuration	New sensors, appliances etc. should easily join the BEMS in order to report energy consumption to the centralized system or even alarms that could be reported locally or remotely	SHOULD
55	Smart plug additional installation in RB	Self-configuration	A dweller should easily and securely include a new smart plug in the system and adjust the level of privacy of its information: no diffusion to community, full diffusion to community, restricted (only diffusion of device type but not of the apartment id for example).	SHOULD
56	Staff connects to the BEMS	Self-configuration	Facility or security staff should easily connect to the BEMS to get the energy consumption information of the building	SHOULD
57	Automatic pairing	Self-configuration	automatic and secure pairing of control appliances module with the IS of the provider, on one hand, and with smart appliances of the home of another hand	SHOULD
59	Service level interfaces having high portability toward the client side	User Interfaces	As described DC6, in order to save energy and money, a customer can choose a service that runs workloads having a medium-low dynamic priority. It's natural that the customer wants to monitor the performance/cost ratio for its workload. To do this is required offer service-level interfaces that works properly on the widest possible range of devices, whether they are fixed or mobile, with different operating systems.	SHOULD

60	End users interface for Office Buildings	User Interfaces	End users of office buildings shall retain control over a limited set of functionalities at local level to some of the systems of the building, without compromising the global energy efficiency strategies set for the whole building. These might include lighting (dimmers, on/off switches), shutter controls, controlled sockets switches, and visualization of energy consumption metering	SHOULD
63	User feedback	User Interfaces	The network must provide a form of user feedback. This can be a return channel in communication or the assured observation of an event by the user	MUST

Table 3: WP4 ICT Requirements Summary

4.4 WP5 – Electric Mobility

The introduction of electric vehicles (EV) will require major changes to be made in electricity networks, as predictions suggest that the charging of electric car batteries will be the biggest load on future networks. Meeting the new demands depends on the introduction of new ICT technology in both the energy grid and the vehicles as well as the connection of the vehicles to the grid in real time. The interaction of EV with the power grid and transport infrastructure needs new innovative services and comes along with significant functional and non-functional ICT requirements. These requirements are to be satisfied with generic and specific enabling technologies.

Therefore a typical set of building blocks for electric mobility should be defined, investigating the interests of a wide range of stakeholders and the likely evolution of their requirements in the coming years as market conditions evolve.

ICT Requirements were be derived from the building blocks that are required from Smart Grids to support the loads that electric vehicles will generate and to balance these loads with the generating ability of renewable energy sources. Additionally, requirements on business models enabling revenue sharing should be defined and detailed requirements for billing and charging systems and security and authentication systems should be compiled.

4.4.1 WP5 Use Cases Summary

4.4.1.1 Use Case Short Trip

The short trip use cases reflect usage of EV for trips within a range of full battery (typically < 150km). The trip destinations are therefore “nearby”, e.g. the place of work, shopping places or places of leisure activities (typically workdays evening or the weekend).

4.4.1.2 Charge Point Accessibility

Functions described herein are derived from 5 different mobility scenarios for medium-ranged distance (< 350 km) trips identified to be important for future electric mobility. All five scenarios are briefly described in the next section.

4.4.1.3 Use Case Long Trip

The basic premises of the Long Trip use cases (ucLT) are that the owner/driver of an electric vehicle will:
a) make long distance journey
b) need to recharge multiple times
c) encounter such roaming issues as availability of charge points and payment options

These use cases include the following four functions:
1. UC-LT-A Authentication
2. UC-LT-IRCP International Roaming Charge Points
3. UC-LT-PM Payment Methods
4. UC-LT-EVC EV User in another country

4.4.1.4 Use Case Grid Operational

While energy suppliers (retailers) can benefit from an extension of their market, grid operators Denial of service (DOS) might be faced with serious problems as to overload situations with parallel charging processes of many electric vehicles (EV). In general terms, DSOs need controlled charge mechanisms). To support those mechanisms and to prevent harmful situations, DSOs might apply the following principles:

- Scenario A: prediction of charge loads – to prepare for stress situations
- Scenario B: optimized charge scheduling – to charge EVs without exceeding the capacity of the local power grid

4.4.1.5 Use Case Value Added Services

This section also assumes that the following electro-mobility key enablers are all in-place and are embedded in national infrastructures. Building on this core set of key enablers, this section tries to identify a number of spin-off value added products and services. It is also assumed that electric vehicles can relatively easily be equipped with these new interactive features and services.

Key enablers include:

- Future electric vehicles will have a high speed wireless internet connection so that the driver / user can receive information on charging stations.
- Future electric vehicles will have a smart device like an iOS, Android, Windows Mobile, QNX, TomTom, Garmin etc. so that the driver / user can visualise maps to closest charging points.
- Future electric vehicles will have embedded geo-location & GPS / Galileo technology so that the driver / user can dynamically plot routes to closest free charging points.
- Data Roaming tariffs will be transparent across Europe and wider countries so that the driver / user can confidently move between states / countries.
- Energy Roaming tariffs will be transparent across Europe and wider countries so that the driver / user can confidently move between states / countries.

4.4.2 Summary of WP5 ICT Requirements before Consolidation

WP5 ID	Name	Category	Short Description	Priorities
1	Interoperability of end points for V2G and G2V	ICT Interoperability	Syntactic and semantic interoperability between all end points in order to guarantee charge point interoperability	MUST
2	Interoperability of the communication between EVs and Charging Stations	ICT Interoperability	Electric Vehicles (EVs) need to exchange data with charge stations, e.g., the current Battery State Of Charge (BSOC) and general technical details such as the maximum charging current. This requires that hardware connections are interoperable and that data exchange protocols and data formats from different EVs can be used at the same charging station.	COULD
3	Interoperability of the communication between EVs and Charging Stations	ICT Interoperability	Electric Vehicles (EVs) need to exchange data with charge stations, e.g., the current Battery State Of Charge (BSOC) and general technical details such as the maximum charging current. This requires that hardware connections are interoperable and that data exchange protocols and data formats from different EVs can be used at the same charging station.	COULD
4	Interoperability of Public Charge Points with EV (ICT and Electrical)	Service Delivery	The charging point supports various models of electric vehicles.	MUST
5	Interoperability of Public Charge Points with EV (ICT and Electrical)	Service Delivery	The charging point supports various models of electric vehicles.	MUST
6	Privacy of user data	Data privacy	The information provided (here: location and planned journey) may not be used by other parties	COULD

7	Privacy of user data	Data privacy	The information provided (here: location and planned journey) may not be used by other parties	COULD
8	Data confidentiality in communication	Security	It shall be possible to ensure the confidentiality of data by cryptographic mechanisms, unless otherwise protected by alternative physical measures. The latency introduced from the cryptographic mechanism shall not degrade the functionality of the system, while the failure of system shall not create denial of service. Data confidentiality here relates to data in transit. This may relate for instance to privacy related data like smart meter information.	MUST
9	Data confidentiality in databases	Security	It shall be possible to ensure the confidentiality of data by cryptographic mechanisms, unless otherwise protected by alternative physical measures. The latency introduced from the cryptographic mechanism shall not degrade the functionality of the system, while the failure of system shall not create denial of service. Data confidentiality here relates to data at rest, i.e., locally stored data needs to be secured appropriately as well. This may relate for instance to privacy related data like smart meter information.	MUST
10	Reliability	Reliability	Data transmission has to be reliable	COULD
11	Reliable data transport over heterogeneous networks	Reliability	Different Communication Service Providers (CSP) are maybe involved in a single data transaction. End-2-End QoS has to be assured over CSP boundaries including identification of Location of Failure.	COULD
12	Healing mechanisms	Reliability	healing mechanisms have to be implemented to keep system in reliable state	COULD
13	Availability	Availability	All ICT infrastructure has to ensure high availability	COULD
14	Availability of Public Charge Points	Service Availability	Public charge points are available to all as many people as possible.	MUST
15	Availability of Public Charge Points	Service Availability	Public charge points are available to all as many people as possible.	MUST
16	Availability of energy prices	Availability	Dynamic energy prices ("Derivation of energy prices") need to be distributed automatically (push) or made available (pull) to charge station providers. In order to facilitate charge station technologies to work with different energy providers, the respective exchange protocols and data formats should be universal.	COULD
17	Availability of grid load information	Availability	Dynamic grid load information ("Forecast of grid loads") need to be distributed automatically (push) or made available (pull) to charge station providers. In order to facilitate charge station technologies to work with different grid operators, the respective exchange protocols and data formats should be universal.	COULD
18	Data integrity	Quality of Service	In particular for all payment scenarios, data integrity has to be ensured.	COULD
19	Data integrity	Security	It shall be possible to ensure the integrity of data and to verify whether the data hasn't been tampered with. The latency introduced from the protection mechanism shall not degrade the functionality of the system. Data integrity relates to data in transit and also data at rest, i.e., locally stored data needs to be secured appropriately. This may relate for instance to data like configuration information.	MUST

20	Low latency of data transmissions for V2G / G2V	Quality of Service	The information exchange for grid stabilizing purpose has to be quasi real-time	COULD
21	Low latency of data transmissions for Stored Energy Services	Quality of Service	The information exchange for grid stabilizing purpose has to be quasi real-time	COULD
22	Remote Upgrade of Infrastructure	Remote accessibility	Required software upgrades of the charging station shall be possible remotely	COULD
23	Remote Upgrade of public charging stations	Remote accessibility	Required software upgrades of the charging station shall be possible remotely	COULD
25	Data management for VAS	System performance	High amounts of data have to be stored and evaluated	COULD
26	Data management for V2G / G2V	System performance	High amounts of data have to be stored and evaluated in order to allow for grid integration services	COULD
27	Scalable computing resources	System performance	Computing resources must be highly scalable in order to process data from Inter-modal Services Users and Inter-modal Mobility Operators	COULD
28	Data throughput for ES	System performance	High data throughput has to be ensured for all kinds of enhanced Services when high numbers of EV are used	COULD
29	Multi-Communication Media	Modularity / Abstraction	For vehicles that are used in different Use Case categories, different communication media may be required (PLC, Wireless, RFID etc.)	COULD
30	Abstraction from Media	Modularity / Abstraction	Despite many different access communication protocols and lots of different hardware solutions, communication must be possible	COULD
31	Data encryption	Security	For all authentication scenarios, the data transmission has to be encrypted	COULD
32	Encryption/Decryption	Security	data traffic encryption for sensible personal data	COULD
33	Code and intrusion protection	Security	Limit possibilities of code/data manipulation	COULD
34	Fault detection	Security	Faults should be detected as early as possible and communicated to given parties	COULD
35	Secure Network Design	Security	The system should restrict the ability of internal or external users to launch denial-of-service attacks against the network components.	MUST
36	System protection (protection against malicious code, like viruses, intrusion prevention, network access control, etc.) which may be host based or network based	Security	The smart grid system shall employ system protection mechanisms. The protection mechanisms shall be deployed in such a manner as to limit the impact of the attack to a small geographical area prior to detection and eradication.	SHOULD
37	Secure Software/Firmware Updates	Security	The system shall ensure software/firmware updates only with integrity protected packages from an authorized source.	MUST

38	Security Management	Security	Security management has to consider all involved cryptographic protection means, including key management infrastructure, certificate management, security policies, addressing both, technical and organizational means. The selection should match the protection needs of the information being protected and the protected system operating constraints.	MUST
39	Data backup and recovery	Security	Backups of critical software, applications, and data for all components of the SCADA system should be assured. Backup should be applied to all data and applications needed to replace failed components within a reasonable period of time as required to satisfy regulatory requirements and to restore the system to normal operation. Backups shall be physically separated from the operational components. Synchronization of the backup and operating data must be assured.	MUST
40	Non-repudiation	Security	It shall be possible to prevent the sender of information from denying sending it.	MUST
42	Identification of End User in front of Public Charge Points	Identification and Authentication	The user identifies themselves to the energy supplier via the charge point.	MUST
43	Unique Identification	Identification and Authentication	Unique Identification per user or car	COULD
44	Identification of End User in front of Public Charge Points	Identification and Authentication	The user identifies themselves to the energy supplier via the charge point.	MUST
45	Authentication and authorization	Security	System components shall uniquely authenticate users and specific components before establishing a connection. The components shall enforce separation of duties through assigned access authorization. The user privileges should be restricted to only those that are required for each person's role, taking into account emergency cases. This reflects least privileged application. Specifically to consider is handling in emergency situations, where a user rights override option should be always implemented. This requires appropriate considerations in the general account policy definition as well as consideration of the specific situation (e.g., by using the simulative information (emergency) as additional parameter for access control) This is to (also) address certain types of DoS attacks.	MUST
46	Storage of Unique Identity	Identification and Authentication	The EV Users unique identity should be stored on a secure card/fob, secure storage on a phone or secure storage on-board the car, with additional cryptographic material for sharing with other systems	SHOULD
47	Transfer of Unique Identity	Identification and Authentication	The EV Users unique identity should be transferred in a secure way over wireless or wire line technologies	SHOULD
48	EVSE Access Codes	Identification and Authentication	Access codes to EVSE's sent over the medium of SMS / email should be unique	SHOULD
49	Open Web Service APIs of network infrastructure	Protocol/Interface	The network infrastructure should feature open web-service API's so that electro mobility cloud services can simultaneously query and reserve both network and cloud services without any human intervention	SHOULD

50	Support of different SLAs of network infrastructure	Quality of Service	The network infrastructure should feature numerous levels of SLA's, the best being guaranteed QoS, the worst being best effort QoS.	SHOULD
51	Fully meshed I/O for P2P in network infrastructure	Performance	The network infrastructure should feature fully meshed i/o's to support advanced peer-to-peer multimedia service applications	SHOULD
52	Network aggregation nodes	Networking	Aggregation nodes are needed in order to use present transport protocols in an efficient way	COULD
53	Provision of Ethernet / IP bandwidth on demand services	Performance	the network infrastructure should support the dynamic and random provision of Ethernet / IP bandwidth on demand services so that high definition uni-cast electro-mobility video services can be enabled on demand	SHOULD
54	Real time billing	Management	converged energy and communications billing systems should support real time billing	SHOULD
55	Billing mechanism: Mobile or m-Payment	Billing and Payment	The EVSE should have a way for completing a mobile, m-payment through a CSP	COULD
56	Billing Mechanism: Access Device	Billing and Payment	The EVSE access device (card/key fob or mobile) holds details on credit amount available to the EV User	COULD
57	Billing Mechanism: Top-Up System	Billing and Payment	The EVSE has a pay as you go system, where the EV User can top their credit on a EVSE Access card	COULD
58	Micro transactional services	Functional	converged energy and communications billing systems should support micro transactional services	COULD
59	Multiple Payment Options at Public Charge Points	Payment	The charge point provides multiple payment options - cash, card, deferred payment (credited to an account).	MUST
60	Multiple Payment Options at Public Charge Points	Payment	The charge point provides multiple payment options - cash, card, deferred payment (credited to an account).	MUST
61	Wireless and fixed architectures	Performance	the network infrastructure should feature a combination of advanced wireless and fixed architectures	SHOULD
62	Wireless coverage	Communication	wireless coverage has to be enhanced in order to dynamically receive information on a journey	COULD
63	Wireless entity connection	Communication	Cars or users must utilize wireless communication infrastructure since they are moving	COULD
64	Simple Communication EV User - Charge Station	Usability	Electric Vehicle Users (EV Users) need to specify preferences such as the Charge Time Frame and the Minimum Battery State Of Charge (BSOC). This can be done in the simplest case by means of a touch screen at the charge station.	COULD
65	Advanced Communication EV User - Charge Station via Virtualization	Performance	The network infrastructure should feature non-blocking advanced virtualization technologies so that many virtual electro-mobility network operators can co-exist on the same physical telecoms network and dynamically scale bandwidth and network services with respect to real-time customer requirements	SHOULD

66	Advanced Communication EV User - Charge Station	Communication	Electric Vehicle Users (EV Users) need to specify preferences such as the Charge Time Frame and the Minimum Battery State Of Charge (BSOC). Instead of simple techniques ("Simple Communication EV User - Charge Station"), this could be done more sophisticated and automatically, e.g., with user-friendly agent technology which could be integrated into a navigation system.	COULD
67	In-Car GUI	Performance	electro mobility services should be interfaced from an in-car GUI	SHOULD
68	Usability	HMI / GUI / Apps	The user interface has to be simple and self-explanatory	COULD
69	App store	Performance	electro mobility application services should be downloaded from a cloud based electro-mobility app store	SHOULD
70	User Context information: EVSE Availability and Tariffs	Information / Data objects	EVSE Availability and Tariffs can be sent to the EV User	COULD
71	User Context information: Battery Information	Information / Data objects	EV on-board battery and auxiliary information can be sent to a storage system	COULD
72	User Context information: Geo-Location	Information / Data objects	An EV Users geo-location information can be sent to a (EV on-board or Online) storage system and can be data mined	COULD
73	User Context information: Profile Information	Information / Data objects	EV User profile information like preferred Electric Power Supplier and preferred tariff/cost per KM can be sent to a storage system	COULD
74	EVSE Context Information: Charge Point Availability	Information / Data objects	The parking bay occupancy status is stored by the EVSE and can be shared with other interested parties	COULD
75	EVSE Context Information: Tariffs	Information / Data objects	Up to the minute energy tariff information is available and can be shared with EV Users	COULD
76	EVSE Context Information: Tariffs	Information / Data objects	Clear information on EVSE booking fees	COULD
77	EVSE Context Information: Capabilities	Information / Data objects	Clear information on EVSE CP capabilities / charging rates (fast charging etc) that can be shared with EV Users	COULD
78	Environmental Context Information: Weather	Information / Data objects	3rd Party services can be accessed for weather information	COULD
79	Environmental Context Information: Traffic	Information / Data objects	3rd Party services can be accessed for traffic information	COULD
80	Environmental Context Information: Landscape Topology	Information / Data objects	3rd Party services can be accessed for landscape/road topology information	COULD
81	Charge Detailed Record	Information / Data objects	The format for a Charge Detailed Record has to be defined	COULD
82	Varying Energy suppliers at one Public Charge Point	Service Delivery	Different energy suppliers use the same charging point to deliver their services.	MUST

83	Derivation of energy prices	Charging and Electricity Grid	Energy providers need to be able to dynamically derive energy prices for the next hours. This requires precise forecasts of the availability of energy, as well as of the expected demand. Dynamic prices are then a means to balance the energy need and to avoid potentially expensive peaks of the demand.	COULD
84	Forecast of grid loads	Charging and Electricity Grid	In electric-vehicle scenarios, unstable electricity grid situations are more likely and they should be avoided. In order to avoid such situations, the grid operators need to be able to precisely forecast the grid load for the next ours. Charge station operators might then react to the current grid situation.	COULD
85	Smart charging scheduling	Charging and Electricity Grid	In a smart-charging scenario, a new (near) optimal schedule needs to be calculated whenever certain parameters change.	COULD
86	Logging and Audit	Security	Logging processes shall be established on devices having appropriate resources. Logging supports security monitoring and auditing.	MUST
87	Time Synchronization	Security	Time synchronization keeps timer elements on different components synchronized.	SHOULD

Table 4: WP5 ICT Requirements Summary

4.5 WP6 – Electronic Market Place for Energy

The high level scenario for an Electronic Market Place for Energy (eMarket4E) arises from the considerations related to evolution of the electricity market due to de-regulation and the transformation of the old electricity grid into a smart grid. In this perspective, a particular attention is for end consumers which now might also produce energy (so called “prosumer”) (e.g., by means of solar panels on the roofs of residential houses or micro-generation plants) and need to be integrated as active elements in the electricity grid.

Anyway, a large variety of actors take part to the Market Place, each having specific needs. In particular, the actors want to boost their business processes by primarily accomplish fruitful transactions. They will deal with various types of assets that can be found in the smart energy market: financial transactions, physical energy capacity commercialization, information services, etc.

The low level scenarios developed in the Electronic Market Place for Energy scenario are grouped together in three clusters (so called “business Cases”):

- Information and final user contracts about energy use - tackles the need of providing to the user the ability to get detailed information about his energy use via different means using the internet in a reliable way as well as to empower the final customer with tools to configure his electricity contract online. It includes the following scenarios which will be described below:
  - Detailed Consumption Information
  - Transparency in the green market
  - Energy contract brokering
  - Information about energy generation sources: Being Green
  - Colour Ethical Bid
- Demand Side Management include a scenario that shows how the final customer is able to get discounts on his electricity bill if he allows the grid users to send signals to his home or premise, in order to flat the Demand curve for example.
  - Flatten Demand Curve
- Energy Trading that represents one of the fundamental pieces of the eMarket4E, it brings together the different actors (grid users, grid operators, providers and customers) of the energy value chain with a particular focus on the involvement of the final energy Customer and Prosumer that at the moment do not have Internet based eMarket4E services for trading. It includes the following scenarios which will be described below:

- Incentive Based Green Market
- Trading for the Good of All
- Trading flexible capacity
- Energy Markets for Neighbourhoods
- Supplier Side Local trading

Here below the low level scenarios have been briefly considered (for more detail about them see D6.1).

4.5.1 WP6 Use Cases Summary

4.5.1.1 Detailed Consumption Information

This scenario deals with the use cases to be considered in FINSENY in the field of eMarket4E services that deal with information closely linked to the energy consumption at the user premises and with tariff schemes. Such services give the users the opportunity to get detailed information of the consumption related to the most consuming devices in their homes. At the same time, the user will be able to get information from the utilities on the tariffs and get energy consumption costs in a granular way.

4.5.1.2 Transparency in the Green Market

The customer, through a smart phone or a PC, accesses the WEB portal of an energy retailer and from there he can plan technically and economically how he would like to contract the energy provisioning service. In this scenario, he would like to measure, in real time, energy costs and monitor the consumption to be able to personalize his contract depending on the costs and program according to his Building Management System (BMS) to comply to the latter.

4.5.1.3 Colour Ethical Bid

In a future smart grids scenario, the final user needs to be aware of the kind of energy that he consumes. In fact, his choices about the consumed kind of energy, contributes to the ecological sustainably in our homes and cities. For that, the final user must know “what kind of energy he is consuming” and “how and where” the waste the elements will be disposed used to produce this energy. To do so, the Energy Information Provider (EIP) provides information to the Customer about the mix of the available energy sources: each kind of energy is represented (on the PC or the smart phone) with a different color (e.g.: red=nuclear, green=renewable, and so on all variations between red and green).

4.5.1.4 Energy Contract Brokering

There is a trend towards the increasing decentralization of energy generation, which manifests itself in the growing number of photovoltaic units, small windmills, combined heat and power plants and other technologies. Today, the operation of such units is often subsidized, but in the long term, such units must be operated in a profit-oriented manner. As supply and demand for electricity must be balanced at all times, it is important that there are mechanisms in place that adapt electricity generation to demand and vice versa (this is achieved through demand side management mechanisms, for example). However, the foundation for direct marketing of electrical energy is a contractual relationship between the supplier and the customer.

4.5.1.5 Information about Energy Generation Sources: Being Green

The scenario consists in getting to the customer via the internet information about the energy that is being generated a given time in relation to their own consumption so they can get statistically if the energy they consumed comes from a “green” (renewable) energy source. Customers will be able to extract the information in various forms and shapes depending on cost and time (e.g. daily consumption, monthly consumption, equivalence in money in CO2).

They will be able to simulate what would be the consumption profile if the energy efficiency system was able to modify the consumption hourly profile to match the green intervals of the Day, Month and Year.

4.5.1.6 Flatten Demand Curve

This scenario describes how an ICT application may contact the customers via a market and effectively manages Distribution System Management (DSM) signals to reduce the power consumption in customer homes.

In this perspective, the user has access to a DSM application on the Internet where he can see different DSM offerings from the grid users and can choose to contract one of these services. This aims at reducing

the monthly bills. By contracting this service, the user allows the grid operator to send DSM signals to his energy efficiency system upon the need to reduce the power consumption in an area, e.g. a region or a city.

4.5.1.7 Incentive Based Green Market

The main scope of this scenario is to spread the participation to the Green Market of the Energy Prosumers providing different kind of incentives. In this perspective, Prosumer negotiates a contract in order to operate on the Green Market with a Grid User who can provide incentives

The Prosumer, according to its own energy production/consumption forecasting, may operate on the Green Market by offering surplus energy while receiving incentives from a Grid User. The Prosumer, who's forecasted energy demand is more than usual, may buy Green Energy receiving incentives, too.

4.5.1.8 Trading for the Good of All

Competition in trading assures energy balancing at city and regional level and guarantees the best price.

In a not so far future scenario on the smart grid, there will be many vendors and consumers of energy, more commonly known as "Prosumers". It's natural that a new energy market will emerge with competition rules in some ways very similar to those of financial markets.

So, in such a scenario, each big Energy Retailer will have at least an Operation Manager that will monitor in real time their "available energy production capacity", and the real cost of such generation. Moreover the Operation Manager gets from a Weather Forecast Service important information useful to plan its future generation capabilities (e.g. for wind or solar energy generation forecasts).

The latter information coming from the Operation Manager is then sent to Financial Managers that, through a WEB portal, continuously monitor in real time the energy price (euro/KWh) of the other supplier competitors and he will thus be able to compare various external offers with his own in terms of availability, costs, and quality. Then he can offer, real time billing to the Final Customer or to the Facility Manager and guarantee is such way short term payments.

4.5.1.9 Trading flexible capacity

This use case describes how ICT infrastructure and market mechanisms can be used for trading the flexible loads for demand side management purposes. The Grid Operator monitors the electricity network using the Network Management System. In case there are overloads or voltage problems detected, the problem is reported to DSM companies through the marketplace. Then, each DSM submits an offer to the marketplace for solving the issue. The marketplace selects a number of offers which jointly solve the network issue. The selected DSMs are now responsible to solve the issue. The objective is to derive real/reactive power changes required to alleviate the violations in the network. The DSM sends the signal to smart home control boxes of his customers. The control boxes send the signal to intelligent devices at the smart home as well as to electric vehicles.

4.5.1.10 Energy Markets for Neighbourhoods

A neighbourhood is a geographically localized community within a larger city, town or suburb sharing a common service infrastructure. In some countries, neighbourhoods are often given official or semi-official status, serving to represent administrative division found immediately below the district level. Generally a neighbourhood is a group of households and public services served by the same local electricity Distribution System Operator (local DSO) which are geographically localized in the same area. Thus, the neighbourhood unit within the project refers to the capability to manage electricity related services. In this way, usually a local DSO will always manage at least one neighbourhood, but there are also cases where a single local DSO manages several neighbourhoods, as it happens nowadays in most cities.

4.5.1.11 Supplier Side Local trading

Taking a closer look to the role of the Supplier, the objective of this scenario is to balance the energy flow among e-Islands, taking into consideration Generators at a regional level. When a deficit/surplus at a local level (e.g. city, regional) occurs, the Supplier can operate on the market to trade energy within the Marketplace either to cover the excess in demand or in production.

A Supplier may want to increase the effectiveness and efficiency of the electricity supply at low voltage level by balancing the energy flow among a controlled e-Islands, taking into consideration small local Generators too. In order to distribute the sufficient amount of energy, a Supplier needs to know the forecast in terms of e-Islands demand/production at different time periods through Microgrid Operators.

When a deficit/surplus occurs, the Supplier has to react and poll the market to trade energy within the Energy Market Service.

4.5.2 Summary of WP6 ICT Requirements before Consolidation

WP6 ID	Name	Category	Short Description	Priorities
1	Access by different connected devices	Service Oriented App.	The contract negotiation should be designed following web-service API, so that different application (including web-based ones) can be developed for different devices.	SHOULD
2	Access by different connected devices	Service Oriented App.	The act of offering energy surplus should be designed by following web-service API, so that different application (including web-based ones) can be developed for different devices.	MUST
3	Access by different connected devices	Service Oriented App.	The act of buying energy surplus should be designed by following web-service API, so that different application (including web-based ones) can be developed for different devices.	MUST
4	Easy-Understand Interface	Usability	The interfaces for all users should be easy-understandable and user-friendly. If not, users would not use the advanced systems.	SHOULD
5	Data integrity	Security/Trust	The transmitted and received data about forecasting of energy demand/production have to be reliable	MUST
6	Privacy of Contract	Security/Trust	The information provided in contract should not be used by other parties	SHOULD
7	Data privacy on energy exchange	Security/Trust	The information provided concerning offering energy surplus should not be used by other parties not participating directly in the eMarketplace4E.	MUST
8	Data privacy on energy exchange	Security/Trust	The information provided concerning buying energy surplus should not be used by other parties not participating directly in the eMarketplace4E.	MUST
9	Easy-Understand Interface	Usability	The interfaces for all users should be easy-understandable and user-friendly. If not, users would not use the advanced systems.	SHOULD
10	Data integrity	Relia/Availability	The data to be transmitted and received have to be reliable in term of truthfulness and timing	MUST
11	Reliability of the system	Relia/Availability	It is very important to guarantee the reliability of the system in term of response time performance	SHOULD
12	Transactional mechanisms	Management	The actions of “offering Energy " and "buying Energy " are meant as ICT transactions between the prosumer and Green Market Operator.	MUST
13	Smart Metering	Physical Media	Microgrid Operators need to have Smart Meters and means to analyze/view the corresponding data in order to be precisely aware of e-Island energy consumption/production.	MUST
14	Transactional mechanisms	Management	The actions of “trading energy” have to be meant as ICT transactions.	MUST
15	Interoperable and standards protocols for forecasting services	Interoperability	Standard interfaces and protocols have to be used, so that aggregation and forecasting services can be easily integrated. Moreover, different providers have to be able to access the marketplace by integrating its own system.	SHOULD
16	Availability/Reliability of forecast in demand/production	Relia/Availability	The Availability of the forecast services have to be high, otherwise energy shortage may happen.	SHOULD

17	Microgrid Management Scalability	Scalability	The management of forecast in demand/production of e-Island has to be designed in a scalable way, as it is expected that the amount of users and thus transactions will increase.	MUST
18	Standardized energy contract	Interoperability	A standard for energy contracts and energy contract offerings need to be available in order to facilitate trading between all actors and to develop tools such as Web-based electronic marketplaces.	SHOULD
19	Marketplace services	Service Oriented App.	An electronic marketplace needs to be available that facilitates the management, negotiation and closing of energy contracts.	MUST
20	Scalability of Marketplace services	Scalability	The Marketplace Services should be offered in a scalable way, as it is expected that the amount of users and thus transactions will increase.	SHOULD
21	Smart Metering	Physical Media	All consumers need to have Smart Meters and means to analyze/view the corresponding data in order to be precisely aware of their energy consumption.	MUST
22	Easy-Understand Interface	Usability	The interfaces for all users should be easy-understandable and user-friendly. If not, users would not use the advanced systems.	SHOULD
23	Data integrity	Relia/Availabilit y	The transmitted and received data has to be reliable.	MUST
24	Privacy of Contract	Security/Trust	The information provided in contracts and offers should not be used by other parties.	MUST
25	Reliability of the system	Relia/Availabilit y	It is very important to guarantee the reliability of the system in terms of response time performance, as users would not use the systems otherwise.	SHOULD
26	Authenticatio n and access control	Security/Trust	All transactions on the marketplace need to be authenticated and the respective users need to have appropriate rights. This requires a role-based access-control system.	MUST
27	Data management and storage	Performance	Large amounts of data need to be collected, stored and made available.	MUST
28	Legally binding electronic contracts	Interoperability	The legal conditions need to allow to electronically close binding contracts, even if they are closed automatically, e.g., by means of intelligent agents.	MUST
29	Transactional mechanisms	Management	Closing contracts should be done giving transactional guarantees.	MUST
30	Standardized grid issue descriptions	Interoperability	A standard for grid issue descriptions need to be available in order to facilitate automated treatment of such situations, e.g., in an electronic market place.	SHOULD
31	Marketplace services	Service Oriented App.	An electronic marketplace needs to be available that facilitates management, collection and selection of grid issues and issue solution (offers).	MUST
32	Scalability of Marketplace services	Scalability	The Marketplace Services should be offered in a scalable way, as it is expected that the amount of users and thus transactions will increase.	SHOULD
33	Smart Metering	Physical Media	All consumers need to have Smart Meters and means to analyze/view the corresponding data in order to be precisely aware of their energy consumption.	MUST
34	Data integrity	Relia/Availabilit y	The transmitted and received data has to be reliable.	MUST
35	Privacy of Contract	Security/Trust	The information provided in contracts and offers should not be used by other parties.	MUST
36	Reliability of the system	Relia/Availabilit y	It is very important to guarantee the reliability of the system in terms of response time performance, as users would not use the systems otherwise.	SHOULD
37	Transactional mechanisms	Management	Closing contracts should be done giving transactional guarantees.	MUST
38	Authenticatio n and access control	Security/Trust	All transactions on the marketplace need to be authenticated and the respective users need to have appropriate rights. This requires a role-based access-control system.	MUST

39	Data management and storage	Performance	Large amounts of data need to be collected, stored and made available.	MUST
40	Availability	Relia/Availability	The availability of all systems needs to be high in order to be able to solve potentially dangerous grid issues immediately.	MUST
41	Electricity Network management	Physical Media	Services for monitoring, supervisory control and operation of electrical networks need to be in place.	MUST
42	Standardized grid issue solution description	Interoperability	A standard for grid issue solutions and grid issue solution offerings needs to be defined in order to facilitate an automated treatment of grid issue situations and to develop tools such as Web-based electronic marketplaces.	SHOULD
43	Control mechanisms for Smart Homes	Protocol/Interface	Standardized mechanisms to control the energy consumption and production in Smart Homes from the outside need to be in place. This includes in particular communication interfaces and a protocol for information exchange.	MUST
44	Control mechanisms in the Smart Home	Protocol/Interface	Standardized mechanisms are needed to control of intelligent devices and electric vehicles within a Smart Home (Internet of Things). This includes all aspects: communication interfaces, network connection for all devices and control mechanisms/information exchange (e.g., balancing signals).	MUST
45	Marketplace services	Service Oriented App.	An electronic marketplace needs to be available that facilitates the management, recommendation, negotiation and closing of energy (shifting) contracts as well as notification services and reporting.	MUST
46	Scalability of Marketplace services	Scalability	The Marketplace Services should be offered in a scalable way, as it is expected that the amount of users and thus transactions will increase.	SHOULD
47	Legally binding electronic contracts	Interoperability	The legal conditions need to allow to electronically close binding contracts, even if they are closed automatically, e.g., by means of intelligent agents.	MUST
48	Smart Metering	Physical Media	All consumers need to have Smart Meters and means to analyze/view the corresponding data in order to be precisely aware of their energy consumption.	MUST
49	Easy-Understand Interface	Usability	The interfaces for all users should be easy-understandable and user-friendly. If not, users would not use the advanced systems.	SHOULD
50	Data integrity	Relia/Availability	The transmitted and received data has to be reliable.	MUST
51	Privacy of Contract	Security/Trust	The information provided in contracts and offers should not be used by other parties.	MUST
52	Reliability of the system	Relia/Availability	It is very important to guarantee the reliability of the system in terms of response time performance, as users would not use the systems otherwise.	SHOULD
53	Transactional mechanisms	Management	Closing contracts should be done giving transactional guarantees.	MUST
54	Authentication and access control	Security/Trust	All transactions on the marketplace need to be authenticated and the respective users need to have appropriate rights. This requires a role-based access-control system.	MUST
55	Data management and storage	Performance	Large amounts of data need to be collected, stored and made available.	MUST
56	Standardized energy information data	Interoperability	A standard for energy information and analytic results needs to be available in order to facilitate the transactions and additional services offered in marketplace as well as energy information analytics for the smart city.	SHOULD
57	Standardized energy contract	Interoperability	A standard for energy (shifting) contracts and energy (shifting) contract offerings need to be available in order to facilitate trading between all actors and to develop tools such as Web-based electronic marketplaces.	SHOULD

58	Energy Monitoring	Physical Media	Mechanisms for delivering data related to the energy consumption and/or production within a Smart House need to be in place for planning, procuring and selling activities. Besides Smart Meters, devices need to be intelligent and to be able to communicate.	MUST
59	Forecast of grid load and energy demand	Management	Reliable forecasts of grid load and energy demand are needed for planning generation and consumption.	SHOULD
60	Rating system	Security/Trust	A rating system is available that facilitates a possibly objective assessment of all marketplace actors. This enables the prosumers to consider them prior to transactions in order to enhance the prosumer's risk management analysis.	SHOULD
61	Info communicatio n system for the Final Users	Service Oriented App.	A WEB portal that allows to the final user, through a smart phone or a PC, to choose between different energy retailer in order to get at best, technically and economically, its energetic needs.	MUST
62	Cloud computing for high speed data processing	Performance	To exchange in real time: pricing Information, present demand, available energy to bid and forecast for the future energy demand, a large amounts of data need to be collected and processed in high speed mode through cloud computing.	MUST
63	Energy Management System	Management	A metering system installed within the final user home and it will be used to measure energy consumed and/or produced	MUST
64	High portability applications for fixed and mobile services targeted to the final customer	Usability	The applications for the services about the eMarket4E have to function properly on the widest possible range of devices, whether they are fixed or mobile, with different operating systems.	MUST
65	Real time system to monitor the available kind of energy for the energy retailers	Service Oriented App.	A SW WEB-based system that allow to the energy retailers to give the kind of requested energy together at all the necessary market information	SHOULD
66	A HW/SW network of grid operators to offer different kind of energy	Management	A network of companies that produce different kind of energy and that sell it at the energy retailer.	SHOULD
67	User Software Agent System	Security/Trust	Autonomous SW entity which observes and stores the final user energy buying habits. Then it acts upon request and directs its activity towards achieving best goals.	MUST
68	Weather Forecast Service	Service Oriented App.	ICT instrumentation that provides services of Weather Forecast to the Operations Manager or to the Energy Information Provider: this can be very useful for to make forecasts about the energy sources depending from wind, sun etc.	MUST
69	Energy information provider	Service Oriented App.	A WEB based information service dedicated to the very small energy retailers providing them the pricing Information, the present local demand and the available energy to bid. Moreover it performs forecasts for the future energy demand coming from the Facility Manager or the Final Customer.	MUST
70	Building data transmission availability	Relia/Availabilit y	The BEMS installed at the user premises will have to transmit data over the Internet. Always on connectivity and ADSL speeds are required and on the provider side (Marketplace) Data Mining will thus apply.	MUST

71	Marketplace services	Service Oriented App.	The service will hold user energy information in detail. And it has to feature the capability of personalizing the interface depending on the context and preferences of the users.	MUST
72	Data Integrity at the Marketplace	Scalability	The Information that is to be collected by the Marketplace has to be handled taking care of personalization and context based information.	MUST
73	Processing capabilities at the Marketplace	Service Oriented App.	The Service at the marketplace will have to implement complex operations between the data that will be collected from the Grid users and operators	MUST
74	Efficient and secure service access and provision	Protocol/Interface	The Ability of generating contracts on the fly over the internet will need to be reliable by employing standard protocols and interfaces for the users. Security access has to be provided also following usual	SHOULD
75	Reliable and deterministic signal commands from the Marketplace	Performance	This UC will need reliable and provisioning QoS, since signalling is involved between the GRID and the user BEMS. The latter signals will have to arrive reliably in order to shape the demand curve.	MUST
76	Real Time Data and Service management	Management	The requirement takes on board the fact that in the future real time tariff schemes will have to be handled by the Market place service.	SHOULD
77	Decision Making and signalling energy commands	Service Oriented App.	The service that may lie on the Grid User side or in the cloud needs to know the user contract and the installed capabilities. According to the latter processing capabilities are key to decide how to signal the shape demand commends.	MUST
78	IPV6 a must for IOT (Customer BEMS and related devices)	Scalability	The BEMS would have to be uniquely identified at the customer premises and in some cases the devices included in energy efficiency services.	MUST
79	Number of customers in the eMarket4E services may grow exponentially	Scalability	The scenario takes into account the customers that may connect to the service. The latter may raise exponentially and thus appropriate data mining data bases must be taken into account. The numbers may raise easily to the hundred thousand.	MUST
80	The Emarket4Eservices availability in a year's time	Relia/Availability	Depending on the scenario there will be more stringent requirements towards availability of the eMarket4E services. DSM will need an availability % of at least 99%.	MUST
81	Speed of communication to the eMarket4E services	Performance	eMarket4E services will require SOTA internet connectivity speeds. In this case speeds starting at 800 Kbps should be provided.	MUST
82	Service Transparency at the customer premises: Data Access	Performance	Emarket4E services will have to access information coming from various devices at the customer premises. Thus Layer 3 protocols should be supported, Access technology agnostic, compatibility with AAA services and also information appliance agnostic.	MUST
83	Ease of use of the eMarket4E services	Usability	The services that will be provided at the eMarket4E will have to comply with: Ease of learning, memorability, maintainability, natural interaction and user satisfaction. This refers to the service interaction design in one side (service provider) and on the other by the artefacts provided at the platform side to mash up and produce services.	MUST

84	Flexibility in the creation of new services interfaces/interaction framework	Usability	Diverse preferences and abilities of the customers should be taken into account when designing the service interaction of eMarket4E services.	MUST
85	Self-configuration for non-networked appliances and physical entities	Self-configuration	Devices and appliances that are monitored and possibly controlled by way of external sensors and actuators (e.g. a smart plug) should be recognized and configured in a way similar to networked devices with zero-conf plug and play mechanisms	MUST
61	Monitoring and control user interfaces for building end-users	User interfaces	User Interfaces for building end-users have to be proposed in at least two different ways : as fixed interfaces inside the building, possibly using a dedicated interface devices (like a home/building control panel), and as either mobile or generic remote interfaces. This duality makes it almost mandatory that the support of these interfaces be available outside of the home network, which will also make it easier for third parties to have access to their own user interfaces	MUST
62	Monitoring, control and management user interfaces for technical staff, facilities managers, etc	User Interfaces	Similar to interfaces for building inhabitants, and excluding the case of homes, these do generally have to be available through fixed or dedicated devices inside the building, and, possibly with reduced functionality, as interfaces outside the building. Similar arguments apply to the support of these interfaces outside the building network.	COULD

Table 5: WP6 ICT Requirements Summary

5. Consolidation Criteria

The previous chapter described the work done by the Use Case Work Packages to generate their use cases and the required ICT requirements to ensure the deployment of the Use Cases. Consequently, the next task was to consolidate these requirements in order to ensure a coherent vision of the needs of all use cases related to the project.

5.1 Categorize and Consolidate ICT Requirements

5.1.1 Categorization

Firstly, it is necessary to identify among the requirements their category, consequently an initial list of categories were suggested that had to be extended depending on the ICT requirements that were identified and documented. The result was a list of category values that includes values related to the perception of the UC about the scope of use case and technical requirements specifications.

The next step was to identify a structure of categories for grouping the categories defined by the UC. Consequently several methods were analyzed and FINSENY decided to use the Schema detailed in the Reference Architecture of the Smart Grid Coordination Group. A specific section of this chapter is devoted to detail the Schema and the Category Layer used for categorization purposes.

Finally, the original categories were grouped according to Layer Categories.

5.1.2 Consolidation

The first step of the consolidation process for the ICT requirements was identifying those requirements that are common. A requirement is common if it was identified in more than one Use Case. For this purpose an analysis of the functional and non-functional descriptions and the original category of each of the requirements were performed.

The second step was to review the common ICT Requirements to identify overlapping or overriding of the requirements. The result was a list of requirements in terms of their impact on different use cases that allows cohesion in the description of the resulting requirements.

An additional purpose of this step was to classify the requirements as essential, non-essential, system level, software level, or as architectural constraints; therefore an initially assigned priority could be reconsidered and re-evaluated.

The last step of the consolidation process was to register the resulting ICT requirements in a new template to allow a direct relationship between the original and consolidated requirements.

Before starting ICT requirements consolidation process an evaluation of the Open Source best practices and the Reference Architecture Working Group of the Smart Grid Coordination group were performed to define the relations related to classification process. The conclusions are summarized in the following sections.

5.2 The Open System Interconnection (OSI)

The Open Systems Interconnection model (OSI model) is a product of the Open Systems Interconnection effort at the International Organization for Standardization. It is a prescription of characterizing and standardizing the functions of a communications system in terms of abstraction layers. Similar communication functions are grouped into logical layers. An instance of a layer provides services to its upper layer instances while receiving services from the layer below.

According to recommendation X.200, there are seven layers, each generically known as an N layer. An N+1 entity requests services from the layer N entity.

Data unit	Layer	Function
Data	7. Application	Network process to application
	6. Presentation	Data representation, encryption and decryption, convert machine dependent data to machine independent data
	5. Session	Inter host communication
Segments	4. Transport	End-to-end connections, reliability and flow control
Packet/Datagram	3. Network	Path determination and logical addressing
Frame	2. Data Link	Physical addressing
Bit	1. Physical	Media, signal and binary transmission

Figure 3: The OSI Model

5.3 Open Security Architecture (OSA)

As is common in many ICT requirements, the distinction between functional and non-functional security requirements of a system is elusive. Security requirements are often discussed in the context of quality and non-functional requirements. Consequently the security requirements are considered only in terms of other requirements to which they are related directly and often handled as an afterthought and add-on to the system's functional requirements.

IT Security Requirements describe functional and non-functional requirements that need to be satisfied in order to achieve the security attributes of an IT system. Security requirements can be formulated on different abstraction levels. At the highest abstraction level they basically just reflect security objectives.

Open Security Architecture (OSA) suggests distinguishing 4 different security requirement types:

- Secure Functional Requirements; this is a security related description that is integrated into each functional requirement. Typically this also says what shall not happen. This requirement artefact can for example be derived from misuse cases.
- Functional Security Requirements; these are security services that need to be achieved by the system under inspection. Examples could be authentication, authorization, backup, server-clustering, etc. This requirement artefact can be derived from best practices, policies, and regulations.
- Non-Functional Security Requirements; these are security related architectural requirements, like "robustness" or "minimal performance and scalability". This requirement type is typically derived from architectural principals and good practice standards.
- Secure Development Requirements; these requirements describe required activities during system development which assure that the outcome is not subject to vulnerabilities. Examples could be "data classification", "coding guidelines" or "test methodology". These requirements are derived from corresponding best practice frameworks like "CLASP".

Consequently, by including a Security Layer to manage security requirements the consolidation process is now able to accurately adapt itself to the current state of the practice of software and ICT requirements integration.

Therefore the Security Layer represents any Information and Communication Technology (ICT) element (Function/Service, Information, Communication and Component) required protecting it from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

5.4 Smart Grid Coordination Group – Reference Architecture Working Group

The Reference Architecture Working Group of the Smart Grid Coordination group, jointly established by ETSI, CEN, CENELEC in response to the M/490 mandate, has the goal to define the Technical Reference Architecture of Smart Grids, *"a technical reference architecture which will represent the functional information data flows between the main domains and integrate many systems and subsystems architectures."* This reference architecture shall be provided in March 2012 (Interim Report) and the final Technical Report by end of 2012. A conceptual model shall be ready by the end of 2011.

5.4.1 Schema of the Reference Architecture

The Reference Architecture Working Group discuss currently a proposal for a universal model for Smart Grid architectures – called at the moment Smart Grid Architecture Model (SGMA) – taking into account the following requirements:

- Being consistent with M490 conceptual model
- Being able to represent the views of different stakeholders in an universal way
- Providing an abstract view on Smart Grid specific structures (domains, scope, layers)
- Being able to represent the current situation and map future concepts (migration)
- Shall be consistent with interoperability categories and with the OSI layer concept

The Smart Grid Architecture Model (SGAM) layers concept can be used as tool for validating smart grid use cases in respect to existing information and communication standards. It can be used for identifying gaps for those circumstances in that a use case is not able to cover all layers or if related components (required to fulfil intended services/functions of an use case) cannot be connected via appropriate physical, communication and information standards under consideration of functional / non-functional requirements. It can also be used to design new smart grid use cases, to study the distribution of functions and their impact on components, information and communication.

In order to validate that existing Smart Grid architectures that can be represented by SGAM layers, the Reference Architecture Working Group mapped it with the ETSI, IEC SG3 Mapping Chart and TC57 Architectures with the following results:

- All representations are similar, the TC57 representation is mostly a flattened version of the layered concept
- New representation concept adds level perspective
- Most of IEC SG3 chart is mapped on Component Layer
- Communication and Information Layers can be filled by specified standards
- Applications in field, station should be specified
- New representation concept adds domain perspective

The FICC Layers allows to represent existing smart grid architectures in a universal way by taking into account the current and future smart grid scenarios and also migration paths, therefore it ensures the validation of smart grid use cases in respect to standards' support and integrates the outcome of the M490 WGs "Sustainable Processes", "First set of standards" and "Security". The SGAM schema is based upon a representation into 3 axes (see Figure 4: SGAM Representation Scheme):

1. **Domains** (i.e. generation, transmission, distribution, …)
2. **Levels of scope** (i.e. process, field, station, …)
3. The following 4 layers:
   - Service/Function Layer
   - Information Layer
   - Communication Layer
   - Component Layer

The SGAM Layers are described as:

- **Service/Function Layer**: Represents logical functions or applications independent from physical implementations
- **Information Layer**: Represents information objects or data models required to fulfill functions and to be exchanged by communication
- **Communication Layer**: Represents protocols and mechanisms for the exchange of information between components

- **Component Layer**: Represents physical devices which host functions, information and communication means

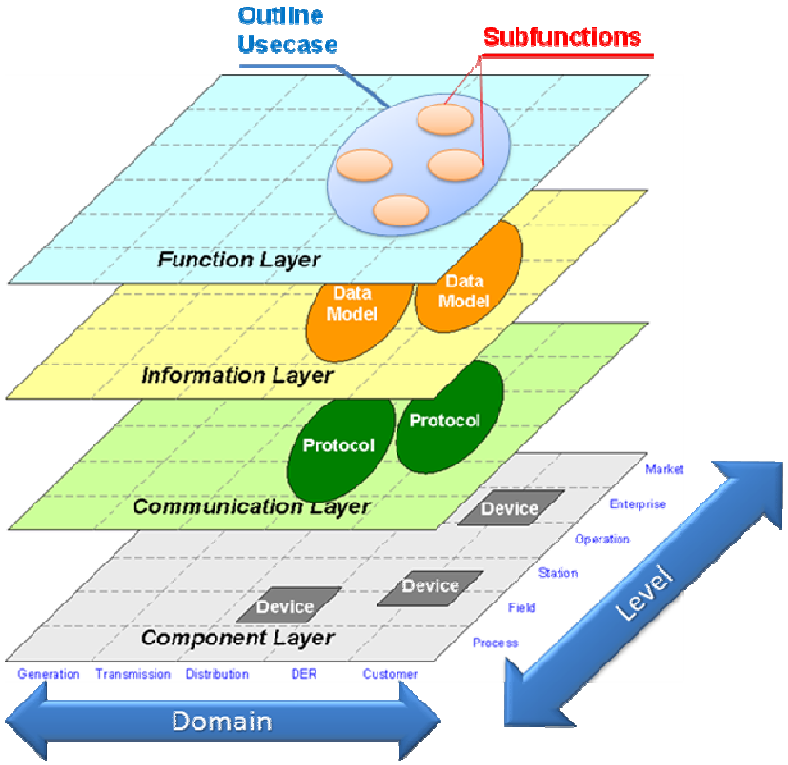

Figure 4: SGAM Representation Scheme

5.4.2 Conclusions

The SGAM Layers are in alignment not only with the EU efforts in the Smart Grid context but also with the most relevant Reference Architectures available today. Moreover, these layers allow defining a configuration category level that is consistent with the methodologies and the work done by different teams in a worldwide scope.

5.5 Security Layer

IT Security Requirements describe functional and non-functional requirements that need to be satisfied in order to achieve the security attributes of an IT system. Security requirements can be formulated on different abstraction levels. At the highest abstraction level they basically just reflect security objectives.

Consequently, by including a Security Layer to manage security requirements the consolidation process is now able to accurately adapt itself to the current state of the practice of software and ICT requirements integration.

Therefore the Security Layer represents any ITC element (Function/Service, Information, Communication & Component) required to protect it from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

5.6 Summary of FINSENY layers

Once the study of the best practices available were finished, the FINSENY project decided to use the FICC Model and take into account the OSA model. Therefore the classification and consolidation of the ICT requirements were done using the following layers:

- **Service/Function Layer**: Represents logical functions or applications independent from physical implementations.
- **Information Layer (OSI layers 6-7)**: Represents information objects or data models required to fulfil functions and to be exchanged by communication.
- **Communication Layer (OSI layers 1-5)**: Represents protocols and mechanisms for the exchange of information between components.
- **Component Layer**: Represents physical devices which host functions, information and communication means.
- **Security Layer (OSA)**: Represents any ITC element (Function/Service, Information, Communication & Component) required to protect it from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

6. ICT Requirements consolidated

This table provides a summary of the current status of consolidation work. It will continuously be improved in an iterative process together with the FI-WARE project and the other use case projects by means of the Fusion Forge tool.

WP ID	Name	Layer	WPs	Short Description	Effort	Priorities	Date	Functional Features	Expected issues
55, 56, 57, 58, 59	Billing and Payment Mechanism	Service/ Function	WP5	The Billing and Payment Systems allows manage the information required by the user to make a transaction.	M	MUST	22/09/11	The EVSE access device (card/key fob or mobile) holds details on credit amount available to the EV User. The EVSE should have a way for completing a mobile; m-payment through a CSP The EVSE has a pay as you go system, where the EV User can top their credit on a EVSE Access card. The charge point provides multiple payment options - cash, card, deferred payment (credited to an account). converged energy and communications billing systems should support micro transactional services	Configuration Security Authentication Accounting Billing Data Management
83	Derivation of energy prices	Service/ Function	WP5	Energy providers need to be able to dynamically derive energy prices for the next hours. This requires precise forecasts of the availability of energy, as well as of the expected demand. Dynamic prices are then a means to balance the energy need and to avoid potentially expensive peaks of the demand.	L	COULD	22/09/11		Deriving energy prices is one of the core challenges of smart energy scenarios. Besides market mechanisms, this requires precise forecasts based on huge amounts of information and intelligent-data-analysis techniques.

84	Forecast of grid loads	Service/ Function	WP5	In electric-vehicle scenarios, unstable electricity grid situations are more likely and they should be avoided. In order to avoid such situations, the grid operators need to be able to precisely forecast the grid load for the next ours. Charge station operators might then react to the current grid situation.	L	COULD	22/09/11		Deriving future grid load prognoses is one of the core challenges of smart-grid scenarios. This requires precise forecasts based on huge amounts of information and intelligent-data-analysis techniques.
85	Smart charging scheduling	Service/ Function	WP5	In a smart-charging scenario, a new (near) optimal schedule needs to be calculated whenever certain parameters change.	S	COULD	22/09/11		This can be done by various existing optimization algorithms. However, it needs to be investigated which algorithms fulfill all requirements (result quality, calculation time etc.).
24	Environmental Requirements for Information and Communication Technology	Service/ Function	WP2	Communication equipment for SG-field-devices / Field Mobile Devices and IT (Servers) operated reliably under different environmental conditions.	M	MUST	11/07/11	SG-related Communication Technology and IT equipment operated reliably in various locations like in - Offices, Data Centers, Sub-Stations (shelter/building) or rural/pole installations, field workers outdoor applications	Limited availability of common communication functions in equipment with extended operating conditions
17	Modularity of Communication Devices	Service/ Function	WP3 WP5	Communication technology is developing rather rapidly. More and more bandwidth will be provided for communication. Wireless reliable secure communication will replace wired communication more and more in the future. It should be easy to replace one communication technology with another one simply by exchanging HW and / or SW modules at the network devices.	L	COULD	05/08/11		
23	Persistent data storage	Service/ Function	WP2	SG devices must contain enough non-volatile memory (e.g. flash memory) for storing measurements, internal data, and enable future firmware and software updates.	L	MUST	08/06/11		This requirement relates to most of the embedded devices of SG system.

22	Future-proof system design requirements	Service/ Function	WP2 WP3	Future-proof system design wrt to modularity, standardization, maintainability and HW/SW upgradeability	M	MUST	11/07/11	Future-proof system design requires modularity, maintainability, upgradeability of hardware, firmware and software as well as long time sourcing	Long time sourcing in contradiction to open market development and semiconductor/parts life-cycle
29	Multi-Communication Media	Service/ Function	WP5	For vehicles that are used in different Use Case categories, different communication media may be required (PLC, Wireless, RFID etc)	M	COULD	22/09/11		
38	High priority asynchronous messages	Service/ Function	WP2	In case of alarms, e.g. in conjunction with power inverters, the according asynchronous messages must be transported very fast to the controller, as alarms normally reflects a very soon loss of energy production. In order to further guarantee the stability of the smart grid, therefore, this information must be transported with highest priority or via reserved communication channels. Without time-synchronization just the priority of the (asynchronous) telegram can be used to reduce the latency from submitting the message until receiving it.	M	MUST	24/06/11	Establish prioritized communication channels Fast priority routing mechanisms Security Means Interoperability of the IT-System on North-bound IT I/Fs. (Wrt processes, applications and databases in the sense of CIM/IEC61968, GID/IEC61970, GIS and Interactions) founded on available standards and extensions. Interoperability on standardized South-bound IT I/Fs as IEC61850, IEC60870, DNP3 used for control and alarm purposes of SG-devices, DER, DG, Storage and SGEC devices.	Reservation of communication channels (hidden to the user) Fast Priority routing Information model interoperability
36, 37	Quality of Service	Service/ Function	WP2	Every network (or network part) should be able to manage differentiated services through the management of priority levels.	M	SHOULD	13/06/11	Application libraries	For some applications priority libraries may not yet exist
21, 20	Low latency of data transmissions	Service/ Function	WP5	The information exchange for grid stabilizing purpose has to be quasi real-time	L	COULD	22/09/11		Not only the data transmission but also the monitoring, the analysis and the derivation of requirements has to be fast enough
50	Support of different SLAs of network infrastructure	Service/ Function	WP5	The network infrastructure should feature numerous levels of SLA's, the best being guaranteed QoS, the worst being best effort QoS.	M	SHOULD	27/07/11		

43	Direct or emergency load control installation	Service/ Function	WP4	automatic and secure pairing of control appliances module with the IS of the provider, on one hand, and with smart appliances of the home of another hand	M	SHOULD	18/09/11		
44	Display installation & configuration	Service/ Function	WP4	automatic and secure pairing of display with meter or meter module, on one hand, and with smart appliances of the home of another hand	M	MUST	18/09/11		
46, 47, 49, 51, 53, 54, 55, 58	Self Configuration for Devices	Service/ Function	WP4, WP6	Any new device that connects to the network must be able to be configured automatically.	M	SHOULD	20/09/11	It should be easy and require no complex configuration to add a new server to the Intelligent Power Node Manager SW and an Energy Management SW of the Data Center It should be easy and require no complex configuration to add a new temperature sensor to the sensor network controlling the Air Conditioning of the Data Center. Can be extended to other sensor types for HVAC system, other component of the energy management system New sensors, appliances etc should easily join the BEMS in order to report energy consumption to the centralized system or even alarms that could be reported locally or remotely A dweller should easily and securely include a new smart plug in the system and adjust the level of privacy of its information : no diffusion to community, full diffusion to community, restricted (only diffusion of device type but not of the apartment id for example).	
48	Energy Management & Optimization System Installation	Service/ Function	WP4	Automatic and secure pairing of control appliances module with the meter or the meter module on one hand, and with smart appliances of the home of another hand.	M	SHOULD	18/09/11		

52	secure connection of BEMS with DR Operator	Service/ Function	WP4	The DR events or dynamic prices must be certified by the originator before being taken into account, so that faked events (or price information) may be dismissed. The verification by the BEMS should require no difficult configuration yet be secure.	M	MUST	18/09/11		
56	Staff connects to the BEMS	Service/ Function	WP4	Facility or security staff should easily connect to the BEMS to get the energy consumption information of the building	L	SHOULD	18/09/11		
57	Automatic pairing	Service/ Function	WP4	automatic and secure pairing of control appliances module with the IS of the provider, on one hand, and with smart appliances of the home of another hand	L	SHOULD	18/09/11		
4, 5	Interoperability of Public Charge Points with EV (ICT and Electrical)	Service/ Function	WP5	The charging point supports various models of electric vehicles.	L	MUST	09/06/11	The charging point must supports various models of electric vehicles or a standard connector must be developed and used on all EVs.	Standardization
82	Varying Energy suppliers at one Public Charge Point	Service/ Function	WP5	Different energy suppliers use the same charging point to deliver their services.	L	MUST	09/06/11		Configuration Security

31, 1, 77, 69, 61, 73, 68, 83	eMarket4E services	Service/ Function	WP6	The services that will be provided at the eMarket4E will have to comply with: Ease of learning, memorability, maintainability, natural interaction and user satisfaction. This refers to the service interaction design in one side (service provider) and on the other by the artifacts provided at the platform side to mash up and produce services.	M	MUST	24/08/11	An electronic marketplace needs to be available that facilitates management, collection and selection of grid issues and issue solution (offers) as well as the management, recommendation, negotiation and closing of energy (shifting) contracts and notification services and reporting. The service also will hold user energy information in detail. And it has to feature the capability of personalizing the interface depending on the context and preferences of the users. A WEB based information service dedicated to the very small energy retailers providing them the pricing Information, the present local demand and the available energy to bid. Moreover it performs forecasts for the future energy demand coming from the Facility Manager or the Final Customer. A WEB portal that allows to the final user, through a smart phone or a PC, to choose between different energy retailer in order to get at best, technically and economically, its energetic needs. The contract negotiation, act of offering energy surplus and act of buying energy surplus should be designed following web-service API, so that different application (including web-based ones) can be developed for different devices.	Standarization
65	Real time system to monitor the available kind of energy for the energy retailers	Service/ Function	WP6	A SW WEB-based system that allow to the energy retailers to give the kind of requested energy together at all the necessary market information	L	SHOULD	26/08/11	The knowledge of the kind of energy should be also available in mobility through the use of Smartphone, laptop, PC, etc. connected to the Internet	this type of information requires a highly secure and fast web service
39	Service discovery mechanism to set appropriate	Service/ Function	WP2	A service discovery mechanism needs to be specified and implemented in order to set the communication network CoS according to the SG-	L	MUST	08/06/11		The service discovery mechanism is required for every service provisioning and usage.

	CoS for communication			devices´ communication requirements.					
18, 25, 26, 27, 28	Data management Performance	Information	WP5	Computing resources must be highly scalable in order to process, storage and evaluate data in order to allow for grid integration services. Data Integrity must be ensured	M	COULD	22/09/11	High data throughput has to be ensured for all kinds of enhanced Services when high numbers of EV are used. Computing resources must be highly scalable in order to process data from Inter-modal Services Users and Inter-modal Mobility Operators	definition of interfaces, both protocol wise and data model wise (could this be simply implemented using cloud technology)
4, 84, 44	Interfaces	Service/ Function	WP2, WP6	The interfaces for all users should be easy-understandable and user-friendly.	M	MUST	22/08/11	Diverse preferences and abilities of the customers should be taken into account when designing the service interaction of eMarket4E services. The interfaces for all users should be easy-understandable and user-friendly. If not, users would not use the advanced systems. The display (HMI) of the grid control application to the grid operator has to be clear and intuitive, providing maximum usability, as it may be used in stressing situations. In case of Demand Side Management, the tariff/price information received from the network has to be understandable both by the automatic home/building energy management system and by the customer (person).	Market and cultural influences
64	High portability applications for fixed and mobile services targeted to the final customer	Service/ Function	WP6	The applications for the services about the eMarket4E have to function properly on the widest possible range of devices, whether they are fixed or mobile, with different operating systems.	L	MUST	20/09/11	This requirement is mandatory because the type of devices used by end users is quite varied: it's the service that must adapt to the customer and not vice versa	Use of non standardized plug-in with compatibility issues.
64	Simple Communication EV User - Charge Station	Service/ Function	WP5	Electric Vehicle Users (EV Users) need to specify preferences such as the Charge Time Frame and the Minimum Battery State Of Charge (BSOC). This can be done in the simplest case by means of a touch screen at the charge station.	XS	COULD	22/09/11		The EV Users might not be able to specify correct Minimum BSOC values. Too large values make smart charging a lot more complicated or even impossible.

27	Topology view	Service/ Function	WP3	Visual view of generation and consumption locations (preferable connection with asset management).		COULD	22/09/11		
59	Service level interfaces having high portability toward the client side	Service/ Function	WP4	As described DC6, in order to save energy and money, a customer can choose a service that runs workloads having a medium-low dynamic priority. It's natural that the customer wants to monitor the performance/cost ratio for its workload. To do this is required offer service-level interfaces that works properly on the widest possible range of devices, whether they are fixed or mobile, with different operating systems.	M	SHOULD	21/09/11	This requirement is recommended because the type of devices used by end users is quite varied: it's the service that must adapt to the customer and not vice versa	Use of non standardized plugin with compatibility issues.
60	End users interface for Office Buildings	Service/ Function	WP4	End users of office buildings shall retain control over a limited set of functionalities at local level to some of the systems of the building, without compromising the global energy efficiency strategies set for the whole building. These might include lighting (dimmers, on/off switches), shutter controls, controlled sockets switches, and visualization of energy consumption metering	L	SHOULD	21/09/11		
61	Monitoring and control user interfaces for building end-users	Service/ Function	WP6	User Interfaces for building end-users have to be proposed in at least two different ways: as fixed interfaces inside the building, possibly using a dedicated interface devices (like a home/building control panel), and as either mobile or generic remote interfaces. This duality makes it almost mandatory that the support of these interfaces be available outside of the home network, which will also make it easier for third parties to have access to their own user interfaces	M	MUST	22/09/11		

62	Monitoring, control and management user interfaces for technical staff, facilities managers, etc	Service/ Function	WP6	Similar to interfaces for building inhabitants, and excluding the case of homes, these do generally have to be available through fixed or dedicated devices inside the building, and, possibly with reduced functionality, as interfaces outside the building. Similar arguments apply to the support of these interfaces outside the building network.	M	COULD	22/09/11		
63	User feedback	Service/ Function	WP4	The network must provide a form of user feedback. This can be a return channel in communication or the assured observability of an event by the user	M	MUST	18/09/11	Feed back	Interaction between different standards, mapping.
7, 8, 12, 13, 14, 43, 24, 25	Device Configuration	Service/ Function	WP2, WP3	When new devices or sub-systems are installed on any point of the Grid they automatically configure itself . Additional Synchronization can be allowed remote control/configuration.	M	MUST	05/08/11	A device or sub-system should be able to describe its capabilities to other entities. A description file is provided by the device and is expressed e.g. in XML. The description file contains information about the device, e.g. its logical devices, functional units and services. The description of the service includes a list of commands and its parameters as well as a list of variables to describe the state of the service at run time.	Standardization of object models for capability description for a large set of devices and properties. NAT, Firewall configuration

13, 16, 17, 16, 17, 40, 16, 70, 80	Availability	Service/ Function	WP2, WP5, WP6	All ICT infrastructure has to ensure high availability	L	COULD	22/09/11	The Availability of the forecast services have to be high, otherwise energy shortage may happen. Dynamic energy prices and grid load information need to be distributed automatically (push) or made available (pull) to charge station providers. In order to facilitate charge station technologies to work with different energy providers, the respective exchange protocols and data formats should be universal. It should be assured (to the most possible extend) that if a component fails, it fails in a manner that does not impact other parts, nor generate unnecessary traffic on the ICS, nor cause another problem elsewhere, such as a cascading event, which would affect other parts and functions. If that cannot be assured a backup/redundancy for the component has to be provided.	Different required levels of availability for different interfaces have to be defined

1	ICT Interoperability	Service/ Function	All	Syntactic and semantic ICT interoperability between all elements of the Grid (HW & SW)	M	MUST	01/04/11	Interoperability on Communication Technology (CT) layer requires utilization of any useful link available under disturbed operating conditions. Central Dispatch System (CSD) and especially Field Mobile Devices (FMD) systems need to support different physical access paths to establish a connection to the CSD´s gateways. These communication links may be utilized: - LTE/4G and UMTS/3G (e.g. for regular operation), - 2G/GPRS – low speed, - Wi-Fi Internet access via Hotspots, - Satellite Links via public or privately operated networks - Direct Ethernet to connect into public networks - Direct Ethernet to connect into substation networks - DSL (ADSL) modem connection to public operators via twisted pairs (assuming no local power, but central office DSLAM power back-up) - Power line communications (PLC/BPL to Low Voltage data networks, i.e. into Smart Meter Field Area Communication networks - FAN) - Local Mesh Radio communications (ZigBee, Z-Wave, i.e. into Smart Meter Field Area Communication networks - FAN)	Standards required to achieve this; many proprietary solutions already exist, others are being designed

66, 26, 40, 63, 59, 76	Grid/Network Management	Service/ Function	WP2, WP3, WP6	The companies responsible for the management of the network must have tools that allow them to handle the available information and predict contingences.	M	MUST	26/08/11	The networking of different kinds of energy requires reliable apparatus that are able to synchronize phases and frequencies to the values provided by the regulations. NMS protocols (e.g. SNMP, at least SNMP v1, SNMP v2 could be supported, SNMP v3 support is desirable.) Visualization tool. Each smart meter has to be connected with a radio device (e.g. ZigBee node) in order to send the collected data in wireless mode. Since almost real-time dynamic tariff schemes should be targeted, data volume will be high, and the management of the related contracts would be demanding because of the potential high amount of users.	This initiative involves the creation of a consortium of producers among them varied for kind of produced energy. Transfer from proprietary to standard database. Forecasting grid load and energy demand is one of the core challenges of smart energy scenarios. This requires huge amounts of historical generation and consumption data and intelligent-data-analysis techniques.
12, 14, 29, 37, 53	Transactional mechanisms	Service/ Function	WP6	The actions of "offering Energy " and "buying Energy " are meant as ICT transactions between the prosumer and Green Market Operator.	L	MUST	22/08/11	The actions of “trading energy” have to be meant as ICT transactions. Closing contracts should be done giving transactional guarantees.	None. Standard mechanisms still exist
65, 69, 35, 62, 31, 51, 67, 30, 31, 51, 67, 28, 29, 34, 53, 75, 82, 81,	Performance Management	Service/ Function	All	Performance management ensures that SLA are being met in an effective and efficient manner. Performance management can focus on the performance of any ICT component of the Grid..	M	MUST	27/07/11	A real time application (like Telecontrol Function) is featured because a delay in the communications has similar effects than a lost. The use of a cloud computing is mandatory to satisfy the high performance needed in this scenario. Using a cloud of HW/SW resources the requested information are so quickly provided to computers and other devices over Internet. Grid users, Service providers and customers would have to connect via web based interfaces to the eMarket4E services.	ICT solution must be designed to have a deterministic behavior. Latency will be the minimum possible for each type of physical medium. Required network latency depends on application implementation and available bandwidth (number and size of messages to be delivered). For remote components there may be no communication medium available.

27, 61, 32									
9, 10, 11, 13, 15, 25, 36, 52	Reliability	Service/ Function	WP2, WP3, WP4, WP5, WP6	Guarantee the reliability of the system in terms of response time performance.	XL	MUST	22/09/11	Workload characterization should exist in order to perform capacity planning studies to ensure desired performance. Different Communication Service Providers (CSP) are maybe involved in a single data transaction. End-2-End QoS has to be assured over CSP boundaries including identification of Location of Failure. The system should be able to identify a loss of the communication systems and be able to switch to a fallback mode.	High cost threat for redundant paths

72	Scalability	Service/ Function	WP2, WP3, WP5 WP6	Scalability is the guarantee that a system can grow without compromising its operations.	M	MUST	09/09/11	Scalability of the IT (central and mobile) systems to allow for system application and I/F-type expansion between Central Dispatch System (CSD) and Field Mobile Devices (FMD) needs: Scalability of the IT systems in terms of - Processing and data base handling capacity and to allow for system expansion incl. - Adaptation to new physical I/Fs: - LTE/4G and UMTS/3G (e.g. for regular operation), - 2G/GPRS – low speed, - WiFi Internet access via Hotspots, - Satellite Links via public or privately operated networks - Direct Ethernet to connect into public networks - Direct Ethernet to connect into substation networks - DSL (ADSL) modem connection to public operators via twisted pairs (assuming no local power, but central office DSLAM power back-up) - Powerline communications (PLC/BPL to Low Voltage data networks, i.e. into Smart Meter Field Area Communication networks - FAN) - Local Mesh Radio communications (ZigBee, Z-Wave, i.e. into Smart Meter Field Area Communication networks - FAN) - New applications, tailored to the above communication capabilities	Security of the information, trust ability. Accessibility.
14, 15	Availability of Public Charge Points	Service/ Function	WP5	Public charge points are available to all as many people as possible.	L	MUST	09/06/11	Distribution of load points based on studies made use.	Standardization Configuration Security

19	Latency	Communication	WP3 WP4	For each Function/Service/Application, the right level of latency must be guaranteed.	L	MUST	05/08/11	Round-trip between service platform (used for remote data processing and storage) and local platform must be strictly bounded for a few safety critical functions	Quality of Service
20	Bandwidth, Throughput, Good put	Communication	WP3 WP4	For each Function/Service/Application, the right level of bandwidth, throughput and good put must be guaranteed.	M	MUST	05/08/11		Quality of Service
21	Request/Response	Communication	WP3	Asynchronous messaging could be needed for some Function/Service/Application. In asynchronous messaging a system places a message in a message queue and does not need to wait for a reply to continue processing.	M	COULD	05/08/11		
1	Error detection, error correction	Communication	WP4	The data link layer must provide sufficient error detection and/or error correction.	S	MUST	18/09/11	ARQ, FEC scheme	Definition of "sufficient" depends on use case, eg. Closed-loop control vs. Light switches.
3	Always on	Communication	WP4	There must be an always on connectivity of selected elements.	M	MUST	21/09/11		Quality of Service
4	Connectivity	Communication	WP4	This requirement relates to the need to “connect” in all relevant senses of the word all devices, appliances, and more generally all physical entities that need to have a network presence inside the extended perimeter of the building management system.	L	MUST	22/09/11	Common Information Model (possibly extending the present IEC CIM) that makes it possible to assign a semantic-level identity to all relevant entities that need to be identified by the building energy management system	need for common information model to be generalized --->will provide shared semantics for all entities to be connected
6	Coexistence of communication standards	Communication	WP4	Several communication standards must be able to coexist on different communication layers.	S	MUST	18/09/11		Existing standards may not be sufficient to guarantee expected QoS
8	Loose coupling	Communication	WP4	The communication protocols used must be as independent as possible from particular energy functions/services/applications.	L	MUST	21/09/11		

22	Remote Upgrades	Communication	WP5	Required software upgrades of the charging station shall be possible remotely.	S	SHOULD	22/09/11		Security issues
52	Network aggregation nodes	Communication	WP5	Aggregation nodes could be used in order to deploy present transport protocols in an efficient way.	L	COULD	22/09/11		communication protocol assessment needs to be done in order to deduce aggregation node locations (heterogeneous landscape)
62	Wireless coverage	Communication	WP5	The level of wireless coverage should be enhanced.	M	SHOULD	22/09/11		Assessment of coverage areas (what is really needed, where and when)
5	Data bus	Information	WP3	Data management is one of the key features of the Microgrid Control Center (MGCC) where high volumes of real-time and historical, static and dynamic operational data are distributed and/or replicated for parallel processing and access. That means up to thousands of data points have to be instantaneously processed, coordinated, manipulated and interpreted if the Microgrid Operator wants to take full advantage of all resources.	M	COULD	02/09/11		
6	Database system	Information	WP3, WP5	Data management including a database system is one of the key features of the Microgrid Control Center where high volumes of real-time and historical, static and dynamic operational data are distributed and/or replicated for parallel processing and access. In an EV environment, a central or local (distributed) database system is required to provide storage system(s) for context information (EV users, EVSE, environmental 3rd party). In	M	COULD	02/09/11	Data has to be stored persistently in a database (e.g. for archiving and post-mortem analysis). The database system has to show high-performance because of the high volume of data and multiple access. Furthermore, the database should support structured and unstructured data and should provide flexible query functionalities. Examples for data storage in the electro mobility environment are: tariffs, battery and auxiliary data, geo-location information. user profiles, weather and topology information etc.	Standardization

				an EVSE, also a local database may be used for charge detailed record.					
9	Distributed Processing	Information	WP3	For balancing supply and demand the Microgrid Control Center has to run the state analysis and define the sub-sequent actions. These tasks include power flow calculations and forecasting models. To minimize processing latency the jobs could be processed in parallel and distributed across different machines. Also for forecasting, planning and revenue in the revenue distributed processing capabilities are crucial.	M	COULD	22/09/11		

10	High Demand for Computing Resources / Processing	Information	WP3	For some use cases, it is necessary to provide high performance computing resources for calculation and simulation models in the Microgrid Control Centre including real-time processing. One example is switching to islanding mode in order to quickly check availability of electrical resources in case islanding of the microgrid is required. Also for long-term planning it may be necessary to provide high performance processing for large-scale planning and simulation. In order to optimize power flow in case of switching to islanding mode, high demand for computing resources for calculation and simulation models in Microgrid Control Centre is required. In order to optimize power flow in case of switching to connected mode, medium processing demand for adaptation to electrical parameters in Overlay Grid is required.	M	COULD	22/09/11		
11	Demand management based on criticality of loads	Information	WP3	MG management and control system shall control loads and enable smart load controlling (cancellation of loads, shifting if loads etc.).	M	COULD	22/09/11		

45	Authentication and authorization	Security	WP2 WP4 WP5 WP6	System components shall uniquely authenticate users and specific components before establishing a connection. The components shall enforce separation of duties through assigned access authorization. The user privileges should be restricted to only those that is required for each person's role (role based access restriction), taking into account emergency cases.	L	MUST	27/06/11	Strong authentication based on asymmetric scheme and credentials, like certificates and corresponding private keys; Simple authentication based on ID and password Secure database Means for RBAC enforcement; Secure key storage	Cryptographic key distribution and revocation Key storage; Handling of failures
46	Data backup and recovery	Security	WP2 WP5	Backups of critical software, applications, and data for all components of the SCADA system should be assured. Backup should be all data and applications necessary to replace failed components within a reasonable period of time as required to satisfy regulatory requirements and to restore the system to normal operation. Backups shall be separated from the operational components. Synchronization of the backup and operating data must be assured.	XL	MUST	27/06/11	Data Synchronization Protection of backups (integrity, in certain cases also confidentiality);	Synchronization of data
47	Data confidentiality	Security	WP2 WP5 WP6	It shall be possible to ensure the confidentiality of the communicated data by cryptographic mechanisms, unless otherwise protected by alternative physical measures. The latency introduced from the cryptographic mechanism shall not degrade the functionality of the system. Data confidentiality relates also to stored data in different type of databases or some devices like ID cards.	L	MUST	08/06/11	Key generation Encryption mechanisms	Some of the equipment, e.g. sensors, may not have enough processing power for data encryption.

48	Data integrity	Security	WP2 WP5 WP6	It shall be possible to ensure the integrity of the communicated data (during the data transfer as well as stored data) and to verify whether the data hasn't been tampered. The latency introduced from the protection mechanism shall not degrade the functionality of the system.	XL	MUST	08/06/11	Creating and checking cryptographic checksum Cryptographic linked lists Mechanisms and Protocols supporting Key generation / Key Management; Secure key storage	Some of the equipment, e.g. sensors, may not have enough processing power for data integrity provision.
49	Non-repudiation	Security	WP2 WP5	It shall be possible to prove that information has been send by a specific source to prevent the sender of information from denying sending it.	L	MUST	27/06/11	Digital signature algorithms (e.g., RSA, ECC based solutions); Hash algorithms (e.g., SHA-1, SHA-256, …); Secure private key storage	Some of the equipment, e.g. sensors, may not have enough processing power for data signing. Decreased performance
50	System protection against malicious code	Security	WP2 WP5	The smart grid system shall employ malicious code protection mechanism. The protection mechanisms shall be deployed in such a manner as to limit the impact of the attack to a small geographical area prior to detection and eradication.	M	MUST	24/06/11	Firewalls, Antiviral software Intrusion Protection Systems / Intrusion Prevention Systems	The antiviral software may increase latency
51	Intrusion detection	Security	WP2	The system shall detect the anomalous events (e.g. meter data alerted) within the network boundaries.	XL	MUST	08/06/11	Intrusion detection systems	The generated alarms may have an impact on the whole energy network, so they shall be screened to determine validity of them before any responsive action is taken.
52	Denial-of-service (DoS) protection	Security	WP2 WP5	The system should restrict the ability of internal or external users to launch denial-of-service attacks against the network components.	XL	MUST	28/06/11	Traffic monitoring and filtering	Increase of latency

53	Cryptographic Key Establishment and Management	Security	WP2	Cryptographic protection and key management infrastructure shall be selected. The selection should match the value of the information being protected and the protected system operating constraints.	XL	MUST	29/06/11	Key generation process Generation algorithms	Key generation, management and periodic changes processes will require additional processing power and support staff.
40	Data privacy	Security	WP4 WP5	In some cases (e.g. the cases discussed in the residential buildings scenarios) stored or processed information while not sensitive (e.g. not health or credit-card related) is still personal and access to it by unauthorized parties would be construed as a privacy infringement reveling the customers daily habits.	M	SHOULD	12/09/11	None	Security, Data Management
41	Workload profiler	Security	WP4	Develops and executes a series of experiments (software simulations) to characterize how much energy capping can be applied to the servers before the performance target is hit. If implemented, this requirement may increase the autonomy of the UPSs in case of blackouts due to fortuitous events or to physical intentional attacks.	M	COULD	16/09/11	To do this requirement, the developers must to perform a series of experiments (software simulations) to characterize how much capping can be applied before the performance target is hit. Afterwards, during normal operations, the applications engineer sets power capping targets based on the prior measurements. The system is now said to be “optimized,” because the impact of the application of these caps is now known.	Great initial manpower effort to characterize each server in different workload conditions
34	Fault detection/monitoring system	Security	WP5	Faults should be detected as early as possible and communicated to given parties. For that reason security monitoring means should be applied.	L	COULD	22/09/11		Fault criteria definition should be extensible in order to react quickly on upcoming issues
37	Secure Software/Firmware Updates	Security	WP5	The system shall ensure software/firmware updates only with integrity protected packages from an authorized source.	XL	MUST	22/09/11	Integrity protection and authentication mechanisms, e.g., digital signatures; Secure key storage	The generated alarms may have an impact on the whole energy network, so they shall be screened to determine validity of them before any responsive action is taken.

38	Security Management	Security	WP4 WP5	Security management policy has to consider all involved cryptographic protection means, including key management infrastructure, certificate management, security policies, addressing both, technical and organizational means.	L	MUST	22/09/11	Key generation process; Key generation algorithms; Certificate and CRL generation; Certificate revocation	Generation, management and periodic change processes will require additional processing power and support staff.
86	Logging and Audit	Security	WP5	Logging processes shall be established on devices having appropriate resources. Logging supports security monitoring and auditing.	S	MUST	22/09/11	Generation and storage of log files; Examination of log files; Protection of log files	Logging and audit will require proper resources and administrational work.
60	Rating system	Security	WP6	To enhance the trust between different business actors of the system, a rating system that facilitates a possibly objective assessment of the actors shall be available. This enables the prosumers to consider them prior to transactions in order to enhance the prosumers risk management analysis.	M	SHOULD	24/08/11		Eliminating fraud in rating systems is challenging and all participants need to actively take part at the system.
13, 21, 33, 48	Smart Metering	Component	WP6	Smart Metering is one of the key functions in Smart Energy Grid scenarios. It allows: all customers to have means to analyze/view the corresponding data in order to be precisely aware of their energy consumption; Grid Users and Grid Operators to actually know close-to-real-time consumption (e.g., to decide on various demand-side and production-management activities) and consequently they are able to know when and how much energy they have to trade in order to improve their business efficiency.	L	MUST	15/09/11		Interoperable standards required to achieve this. Regulations might differ in different countries.

58	Energy Monitoring	Component	WP6	Mechanisms for delivering data related to the energy consumption and/or production within a Smart House need to be in place for planning, procuring and selling activities. Besides Smart Meters, devices need to be intelligent and to be able to communicate.	M	MUST	24/08/11		Standards required to achieve this; many proprietary solutions already exist, others are being designed.
43, 44	Control mechanisms for Smart Homes	Component	WP6	Standardized mechanisms need to be in place in order to: control the energy consumption and production in Smart Homes from the outside; control intelligent devices and electric vehicles within a Smart Home (Internet of Things domain). These mechanisms include in particular communication interfaces, a protocol for information exchange, network connection for all devices and control mechanisms/ information exchange (e.g., balancing signals).	L	MUST	24/08/11		Standards required to achieve this; many proprietary solutions already exist, others are being designed.
74	Efficient and secure service access and provision	Component	WP6	The Ability of generating contracts on the fly over the internet will need to be reliable by employing standard protocols and interfaces fro the users. Security access has to be provided also following usual	L	SHOULD	09/09/11	The service will need to follow Web 2.0 guidelines and openness. Mostly Web-based interfacing technologies will be used.	Effective interface with adaptability per user basis (Context). Certification.
9, 27	Local processing and storage	Component	WP4	Data processing and storage requirements are indispensable for any sort of building-level intelligence and so to inform the consumers about the building status (through a human-machine interface) or to communicate with the grid (through an interoperability interface). See more extended discussion in referenced document.	M	MUST	12/09/11	Support for on the fly remote configuration	Data Management

10, 11, 12	Remote processing and storage	Component	WP4	The platform must offer a way for calculating aggregated consumption, energy-related data and costs for homes and buildings with the same profile. Moreover, the consideration of demand-shaping measures and the implementation of peak-shaving capabilities require the grid administrator to have some sort of further data access. Concretely, it is necessary to maintain information about the contract model of each subscriber, the options available to that model, and the extent to which some of these options have already been used.	M	MUST	12/09/11	Define logical model for remote data that needs to be stored in the cloud. Allow the logical model to be extensible so as to accommodate future requirements. Main concepts to model: subscriber, contracts, incentives and counter-incentives for the implementation of peak shaving features.	Data Management
18	Dedicated or Shared Transport Infrastructure	Component	WP2	Control from an Aggregator, VPP or DSO needs appropriate transport network capacity, which may be supplied by a dedicated operator on an exclusive or shared basis	S	MUST	04/07/11	South-bound IT (Server) I/Fs need to connect via suitable transport links towards the SG-device locations (e.g. Sub-Stations) Transport links may be realized via: - Optical Fibers, operating WDM, SDH/PDH, Ethernet/LAN, - 3GPP-defined cellular wireless (2G/GPRS 3G/UMTS 4G/LTE) - WIMAX or Microwave private radio network - Powerline based PLC/BPL (Powerline/Broadband Powerline Communication) - Commercial DSL-lines based on ADSL, VDSL or SHDSL	None, but eventually high maintenance effort to fulfill SLAs

19	Dedicated or Shared Transport Infrastructure 2	Component	WP2	The Communication Technology (CT) layer requires utilization of any useful link available under disturbed operating conditions. This may be supplied by a dedicated operator on an exclusive or shared basis	M	COULD	11/07/11	These communication technologies may be utilized: - LTE/4G / WiMAX - Satellite Links - Direct Ethernet to connect into substation networks - Powerline communications (PLC/BPL to Low Voltage data networks, i.e. into Smart Meter Field Area Communication networks - FAN) - Local Mesh Radio communications (ZigBee, Z-Wave, i.e. into Smart Meter Field Area Communication networks - FAN)	None, but eventually high maintenance effort to fulfill SLAs
20	Telco Infrastructure	Component	WP2	Control from an Aggregator, VPP or DSO needs appropriate transport network capacity, which may be supplied by a Telco operator	L	COULD	04/07/11	South-bound IT (Server) I/Fs need to connect via suitable transport links towards the SG-device locations (e.g. Sub-Stations) Transport links may be realized via: - 3GPP-defined cellular wireless (2G/GPRS 3G/UMTS 4G/LTE) - WIMAX public radio network - Public DSL-lines based on ADSL, VDSL or SHDSL	Precautions may need to be taken to reach desired reliability and security
21	Telco Infrastructure 2	Component	WP2	The Communication Technology (CT) layer requires utilization of any useful link available under disturbed operating conditions. This may be supplied by a Telco operator.	L	COULD	11/07/11	These communication technologies may be utilized: - LTE/4G and UMTS/3G (e.g. for regular operation), - 2G/GPRS – low speed, - WiFi Internet access via Hotspots, - Satellite Links - Direct Ethernet to connect into public networks - DSL (ADSL) modem connection to public operators via twisted pairs (assuming no local power, but central office DSLAM power back-up)	Enablement of various gateways to public network may be difficult to negotiate

49, 41	Web-Service-enabled technologies for electricity network management	Component	WP5, WP6	Services for monitoring, supervisory control and operation of electrical networks need to be in place. The network infrastructure should feature open web-service APIs so that electro mobility cloud services and marketplace services can simultaneously query and reserve both network and cloud services without any human intervention.	L	MUST	27/07/11		As electricity networks are complex, data from many different sources need to be integrated and means for controlling individual entities in the network need to be in place. This involves various aspects of security.

7. Conclusion

For the management of the Use Cases and the generation of the ICT requirements the FINSENY project relied on the IntelliGrid methodology that was adequate to the specific characteristics and needs of this project.

The ICT Requirements defined and detailed by the Use Case Work Packages were merged and classified according to their initially categories identified and the functional and non-functional characteristics.

A Category Layer for consolidation purposes was defined using the FICC Schema defined by the Reference Architecture Working Group of the Smart Grid Coordination Group of CEN/CENELEC/ESI and an additional layer, “Security” were included too.

8. Terms and Abbreviations

A&A	Authentication and Authorization (Access Control)
ADSL	Asymmetric Digital Subscriber Line
AES	Advance Encryption Standard
APDU	Application Protocol Data Unit
API	Application Programming Interface
BCP	Business Continuity Plan
BDSG	Bundesdatenschutzgesetz/German Data Protection Act
CAPEX	Capital Expenditures
CoS	Class of Service
CRC	Cyclic Redundancy Check
CSD	Central Dispatch System
CSP	Communication Service Provider
CT	Communication Technology
DAC	Data Acquisition and Control
DB	Database
DCAC	Dynamic Control of Active Components
DiffServ	Differentiated Services
DMZ	Demilitarized Zone
DN	Distribution Network
DNO	Distribution Network Operator
DoS	Denial of Service
DSA	Digital Signature Algorithm
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DSO	Distribution System Operator
EAL	Evaluation Assurance Level (Common Criteria Evaluation)
ECC	Elliptic Curve Cryptography
EG1	Expert Group 1 (of SGTG)
EMI	Electro-magnetic Interference
EPRI	Electrical Power Research Institute
ERGER	European Regulators Group for Electricity and Gas
ERP	Enterprise Resource Planning
ESCO	Energy Service Company
ESD	Electro-static Disturbance
EV	Electric vehicle
EVSE	Electric Vehicle Supply Equipment
FAN	Field Area Network
FERC	Federal Energy Regulatory Commission
FERC	Federal Energy Regulatory Commission
FI	Future Internet
FINSENY	Future INternet for Smart ENergY
FI-PPP	Future Internet Public Private Partnership
FI-WARE	Future Internet Ware (Technology foundation: Future Internet Core Platform)
FLIR	Fault Location, Isolation and Service Restoration
FMD	Field Mobile Devices

FRT	Fault Ride Through
GPRS	General Packet Radio Service
GUI	Graphical User Interface
HMI	Human Machine Interface
HW	Hardware
IATF	Information Assurance Technical Framework
IATF	Information Assurance Technical Framework
ICS	Information and Communication System
ICT	Information and Communication Technology
ID	Identifier
IDS	Intrusion Detection System
IEC	International Electrotechnical Comission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IS	Information Security
ISO	International Standardization Organization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
LAN	Local Area Network
LDAP	Local Directory Access Protocol
LTE	Long Term Evolution
MIB	Management information base
MPLS	Multiprotocol Label Switching
MTBF	Mean Time Between Failures
MTTR	Maximum Time to Repair
MV	Medium Voltage
MVDAC	Medium Voltage Data Acquisition and Control from utility control centre
MWFM	Mobile Work Force Management
NIST	National Institute of Standards and Technology
NMS	Network Management System
OPEX	Operational Expenditures
PAS	Publicly Available Specification
PC	Personal Computer
PDH	Plesiochronous Digital Hierarchy
PKI	Public Key Infrastructure
PLC	Power Line Communication
QoE	Quality of Experience
QoS	Quality of Service
R&DD	Research, Development and Demonstration
RSA	Rivest, Shamir, Adleman, cryptographic algorithm allowing signature and encryption
RTU	Remote Terminal Unit
SAML	Security Assertion Markup Language
SANS	SysAdmin, Audit, Network, Security
SDH	Synchronous Digital Hierarchy
SDL	(here: Microsoft) Security Development Lifecycle

SEG	Smart Energy Grid
SG	Smart grid
SGEC	Smart Grid Energy Control of Power Grid
SGTF	Smart Grid Task Force (DG Energy)
SHDSL	Single-pair High-speed Digital Subscriber Line
SHG	Self-Healing Grid
SLA	Service Level Agreement
SM	Smart Meter
SML	Strength of Mechanism Level (IATF)
SNMP	Simple Network Management Protocol
SQL	Structured Query Language (DB access)
SSL	Secure Socket Layer (kind of TLS)
SW	Software
T & R	Threat & Risk (Analysis)
TDM	Time Division Multiplex
TLS	Transport Layer Security
TNO	Transmission Network Operator
TSO	Transmission System Operator
UC	Use Case
UMTS	Universal Mobile Telecommunications System
VAR	Volt Ampere Reactive
WDM	Wavelength Division Multiplexing
WP	Work package

9. References

- FINSENY Internal Reports: IR2.1, IR3.1, IR4.1, IR5.1 & IR6.1
- Open Security Architecture (OSA) - http://www.opensecurityarchitecture.org
- Open System Interconnection - http://en.wikipedia.org/wiki/OSI_model
- ISO/IEC 7498-1:1994, Information technology—Open Systems Interconnection—Basic Reference Model: The Basic Model
- ITU-T Recommendation X.200 (11/93) [ISO/IEC 7498-1:1994], Open Systems Interconnection - Basic Reference Model.
- M/490 Reference Architecture WG – 02/09/2011 – Smart Grids CG – Reference architecture WG - © CEN-CENELEC-ETSI 2011
- Communication architecture for the Smart Grid - P Wetterwald, J Heiles, R Forbes, O Elloumi
- IEC TC57 Reference Architecture –Scope and Layers – www.iectc57.ucaiug.org
- Standardization and Requirements: Methodology for comparison – PlasTEP
- Security Quality Requirements Engineering (SQUARE) Methodology - Nancy R. Mead, Eric D. Hough, Theodore R. Stehney II - November 2005
- Towards a Goal-Oriented Requirements Methodology based on the Separation of Concerns Principle - Geórgia Maria C. de Sousa and Jaelson Brelaz de Castro - Centro de Informática – Universidade Federal de Pernambuco (UFPE) - Caixa Postal 7851, CEP: 50.732-970, Recife – PE – Brasil
- Agile Methodology in Requirements Engineering – Sujoy Bose, Manish Kurhekar and Joydip Ghoshal – SETlabs Briefings Online – 2008
- PDM: A requirements methodology for software system enhancements - R. G. Mays, L. S. Orzech, W. A. Ciarfella, R. W. Phillips – IBM Systems Journal – Volume 24, Number 2
- Recommendations for the Description and Management of Use Cases for Smart Grids - DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik – José M. Gonzalez, Jörn C. Trefke - Version of 28.02.2011
- IntelliGrid Methodology for Developing Requirements for Energy Systems - INTERNATIONAL ELECTROTECHNICAL COMMISSION - ISBN 2-8318-9525-1 - Edition 1.0 2008-0
- IEC Smart Grid Standardization Roadmap - SMB Smart Grid Strategic Group (SG3) - June 2010; Edition 1.0
- Agile Requirements Modeling - http://www.agilemodeling.com/
- Beywatch European project – ICT for energy efficient Homes and Neighbourhoods – http://www.beywatch.eu/
- GridWise Architecture Council (GWAC) - http://www.gridwiseac.org/

Annex I – WPs ICT Requirements

FINSENY Template

The following table is a summary of the ICT Requirements identified by WP.

Id	Name	Category	WP	UC #	Description	Eff.	Priority	Justifications
1	Interoperability on IT (Server) level	Interoperability	WP2	SGEC DCAC MVDAC FLIR	Interoperability on - North-bound IT I/Fs between DSO, Aggregator and VPP wrt process and application data and database formats - South-bound IT I/Fs wrt device information models	M	MUST	Interoperability on IT level is relevant for a standardized operation and data exchange in operating Aggregator, VPP and DSO environment and for equipment vendors.
2	Interoperability on IT (Server) level 2	Interoperability	WP2	MWFM	Interoperability between - Central Dispatch System IT I/Fs and - Field Mobile Devices (Smart Phone or/and laptop) wrt process and application data and database formats utilizing various communication links	L	COULD	Interoperability for MWFM is relevant for operation and data exchange under critical situations, where regularly used communication methods are disturbed
3	Interoperability on Communications Technology (CT) layer	Interoperability	WP2	SGEC DCAC MVDAC FLIR	Interoperability on - North-bound CT I/Fs between DSO, Aggregators and VPPs wrt intra and inter-company communication - Standardized South-bound I/Fs wrt SG-devices communication	M	MUST	Interoperability on CT layer is relevant for a standardized operation and data exchange of SGEC, DCAC, MVDAC and FLIR related information
4	Interoperability on Communications Technology (CT) layer 2	Interoperability	WP2	MWFM	Interoperability on Communication Technology (CT) layer requires utilization of any useful link available under disturbed operating conditions.	L	COULD	Interoperability for MWFM is relevant for operation and data exchange under critical situations, where regularly used communication methods are disturbed

5	Time Synchronization	Interoperability	WP2	SGEC DCAC MVDAC FLIR MWFM	Today the Internet does not show any deterministic behavior. However, within a smart grid measurement values are transported which could require a fast transport (e.g. phase measurements). Also alarm signals sent out by components should arrive to the components´ controller with low latency. In order to achieve this the following methods could be applied: In case of scheduled actions a time based planning of the communication could further optimize the communication load within the communication network, as there are (in ideal case) no collisions will occur. This could be achieved by setting up a planning of telegram slots. The control of the components in the grid is then done using a time-slot-controlled data-/telegram transfer. It would be enough to reserve some slots for the above mentioned cases (alarm, high dynamic measurement values). The necessary number of reserved channels depends on the MTBF of the network (because the number of alarms relates to the MTBF). In case that planning is not set in place a time-stamped telegram could be used in order to interpret e.g. metering data in a more precise way. However, that method is maybe not good enough for alarms. But in both cases the deterministic of the communication network is enhanced. Reserved time-slots are normally realized by synchronization of all time-bases which are present in the various components of the grid. That synchronization could be done on various ways. One way is to use the time signals which are spread via satellites or terrestrial broadcast.	M	MUST	Without clock controlled communication the above mentioned advantages cannot realize, and the communication network cannot operate in the intended optimized way.
6	Scalability on IT (Server) level	Scalability	WP2	SGEC DCAC MVDAC FLIR	Scalability of the IT systems and their I/Fs to allow for system expansion	L	MUST	

7		Scalability	WP2	SGEC DCAC MVDAC FLIR	Scalability of communication networks connecting - North-bound IT I/Fs (Enterprise Bus) between DSO, Aggregators and VPPs incl. intra and inter-company connections - South-bound IT I/Fs to SG-devices	S	MUST	Scalability on CT layer is relevant for a standardized operation and data exchange of SGEC related information.
8	Scalability on IT (Server) level and Communications Technology (CT) layer	Scalability	WP2	MWFM	Scalability of the IT (central and mobile) systems to allow for system application and I/F-type expansion between Central Dispatch System (CSD) and Field Mobile Devices (FMD).	XL	COULD	
9	Reliability and availability on IT (Server) level	Reliability and availability	WP2	SGEC DCAC MVDAC FLIR	Reliability of IT operations towards Aggregator, VPP or DSO processes, applications, databases and SG-devices.	M	MUST	Defining availability figures on IT level is relevant for ongoing operation and also related to safe grid operation.
10	Reliability and availability on Communications Technology (CT) layer	Reliability and availability	WP2	SGEC DCAC MVDAC FLIR	Reliability of CT layers I/Fs towards Aggregator, VPP or DSO and SG-devices.	M	MUST	Defining availability figures on CT layer is relevant for ongoing operation and also related to safe grid operation
11	Handover Management	Reliability and availability	WP2	MWFM	The communication handset device used by field worker to synchronize work orders should have the availability to manage the handover between several commutations media in a transparent way. The best media should be selected regarding the QoS needed in term of latency, jitter and bandwidth. In case of a crisis situation (a tempest for example), a crisis media (such as Private Mobile Radio) should be available for data communication with the same handset device used by workers during “normal” situation.		SHOULD	Multihoming with automatic handover management will enhance the possibility for a worker to have access to central data, especially in a crisis situation
12	IP mobility	Reliability and availability	WP2	MWFM	From the Dispatch System point of view, the communication system must be able to “push” data to the worker handset whatever the telecommunication medium the worker is currently using, even if its IP address has changed.		SHOULD	IP mobility is an issue that must be handled by the communication system
13	Adaptation of application to available bandwidth	Reliability and availability	WP2	MWFM	If a low bandwidth media is used (for example in the case of a crisis situation after a tempest), the central IS Dispatch System must adapt its response according to the bandwidth available: only the core data of the work order are sent and not the attached files.		SHOULD	Application plasticity will be very helpful especially during crisis situation in order to be able to send data to the field workers.

14	Scheduled actions	Reliability and availability	WP2	SGEC DCAC	Scheduled actions are to be used to transmit automatically a pre-defined set of data to and/or from the power site (e.g. power inverter) without sending messages for ordering that data in before. Such data could be regular status information, metering data, meteorological data, etc. If the transmission time is not deterministic a time-stamp should be part of the transmission.	M	SHOULD	Automated and synchronized background processes are serving for optimized communication loads which are necessary to successfully operate a smart grid.
15	Failsafe Mechanisms	Reliability	WP2	SGEC DCAC MVDAC FLIR	As stated in the power inverter use-case description, the inverter can have different communication partners (TSO, DSO, Aggregator, Virtual Power plant ...). However, just one communication partner ("Controller") is allowed to control the inverter, but several communication partners could be simultaneously informed about the status of the inverter and/or additional information like metering and/or forecast data.	M	MUST	Flexibility in Login and Logout of DER must be possible in order to keep the smart grid as flexible as possible. This includes re-routing to another controller in case of communication / unit failures of the dedicated communication partner/controller (Note: Re-routing of connections between that partners is already given, e.g. in case of a router is inactive the metering data will be re-directed to another router but is still received by the same unit. However, now the control task must be shifted, too).
16	Backup of communication links	Availability	WP2	SGEC DCAC MVDAC FLIR	Backup solution should be provided for the communication links. Interfaces enabling communication should operate also at the time when the DSO grid is down. Exception can be a LV PLC link.	L	COULD	The communication may be necessary for grid re-establishing.
17	Single point of failure avoidance	Availability	WP2	SGEC DCAC MVDAC FLIR	It should be assured (to the most possible extend) that if a component fails, it fails in a manner that does not impact other parts, nor generate unnecessary traffic on the ICS, nor cause another problem elsewhere, such as a cascading event, which would affect other parts and functions. If that cannot be assured a backup/redundancy for the component has to be provided.	L	COULD	Redundancy is needed for critical components which will affect the whole system when failing.
18	Dedicated or Shared Transport Infrastructure	Physical Media	WP2	SGEC DCAC MVDAC FLIR	Control from an Aggregator, VPP or DSO needs appropriate transport network capacity, which may be supplied by a dedicated operator on an exclusive or shared basis	S	MUST	Transport infrastructure is relevant for ongoing SG operation, private or dedicated networks may be purpose designed (for reliability, security)

19	Dedicated or Shared Transport Infrastructure 2	Physical Media	WP2	MWFM	The Communication Technology (CT) layer requires utilization of any useful link available under disturbed operating conditions. This may be supplied by a dedicated operator on an exclusive or shared basis	M	COULD	Transport infrastructure is relevant for ongoing SG operation, private or dedicated networks may be purpose designed (for reliability, security)
20	Telco Infrastructure	Physical Media	WP2	SGEC DCAC MVDAC FLIR	Control from an Aggregator, VPP or DSO needs appropriate transport network capacity, which may be supplied by a Telco operator	L	COULD	Transport Infrastructure is relevant for ongoing SG operation, pervasive public networks don't require high CAPEX and prospect lower OPEX due to shared utilization
21	Telco Infrastructure 2	Physical Media	WP2	MWFM	The Communication Technology (CT) layer requires utilization of any useful link available under disturbed operating conditions. This may be supplied by a Telco operator.	L	COULD	Transport Infrastructure is relevant for ongoing SG operation, pervasive public networks don't require high CAPEX and prospect lower OPEX due to shared utilization
22	Future-proof system design requirements	Future-proof system	WP2	SGEC DCAC MVDAC FLIR	Future-proof system design wrt to modularity, standardization, maintainability and HW/SW upgradeability	L	MUST	Functional architecture may become dependent on practically available equipment which is compliant to operational conditions
23	Persistent data storage	Future-proof system	WP2	SGEC DCAC MVDAC FLIR MWFM	SG devices must contain enough non-volatile memory (e.g. flash memory) for storing measurements, internal data, and enable future firmware and software updates.	L	MUST	
24	Environmental Requirements for Information and Communication Technology	Environmental	WP2	SGEC DCAC MVDAC FLIR MWFM	Communication equipment for SG-field-devices / Field Mobile Devices and IT (Servers) operated reliably under different environmental conditions.	M	MUST	Functional architecture may become dependent on practically available equipment which is compliant to required operational conditions
25	Availability in end points	Performance	WP2	MVDAC	Availability in end points	XL	COULD	When Tele control function is unavailable, only local control is allowed. Local control implies field workers local assistance for taking any measurement and making any orders This local assistance is more expensive, require much more time and is less safe.

26	Availability in central points	Performance	WP2	MVDAC	Availability in central points	XL	COULD	A utility control centre cannot become unavailable for no reason. If there are any incidents that affect only to the control centre location, there are emergency control centre locations where grid operators must move as soon as possible. This emergency control centre rests over the same central points indicated before.
27	System availability	Performance	WP2	FLIR MWFM SGEC DCAC	Non critical components: 99.5% + availability System-critical components: 99.9% +		COULD	To avoid outages and guarantee fast restoration in case of faults the systems for FLIR, MWFM and control (SGEC, DCAC) must have high availability.
28	Maximum Time to Repair (MTTR)	Performance	WP2	MVDAC	Maximum Time to Repair	L	COULD	When Tele control function is unavailable, only local control is allowed. Local control implies field workers local assistance for taking any measurement and making any orders This local assistance is more expensive, require much more time and is less safe.
29	Mean Time Between Failures (MTBF)	Performance	WP2	MVDAC	Mean Time Between Failures	L	COULD	Any failure, even that it is solved in a short period, spent a lot of resources in both the client and the provider.

30	Latency	Performance	WP2	FLIR MWFM SGEC DCAC	The communication infrastructure must offer a guarantee on the maximal round trip time for messages (from the application on the originator device to the destination device and back)	L	COULD	FLIR: In order to comply with standards (CEI, IEEE) FLIR is required to complete restoration within one minute. Since several messages have to be disseminated during the process, a delay of at most one second is acceptable. For teleprotection a delay of at most 50ms must be guaranteed. Since the voltages are much lower in the distribution network than in the transmission network, teleprotection is less important here than in transmission networks and we can omit the harsh requirement that only <50ms latency is acceptable (nice to have, but requires a large effort). MWFM: To react timely to new situations, field workers need to be notified of important events within seconds DCAC, SGEC: Control applications require fine-grained updates on state and fast delivery of commands, the typical latency requirement is one second. Some system critical components might require faster communication for network stability.

31	Delay and Jitter	Performance	WP2	MVDAC	Delay and Jitter must be controlled for Tele control Function	XL	COULD	As an example, the Tele control Function is implemented by means of a periodical polling, each 2 seconds. This period is related mainly by the latency of the physical medium. When using specific physical mediums for example geostationary satellite mediums, these periodical polling should be longer (each 3 seconds for example). The effect of this is that when a grid operator sends an order, receives the updated information in the grid control application in less than this configured period. Jitter must be controlled in any case. When an answer arrives after the periodical polling period, a communication error arises. It has the same effect than a communication lost.
32	Bandwidth	Performance	WP2	MVDAC	Bandwidth requirements for MV secondary substations	XL	COULD	Strict priority bandwidth guaranteed is required for Tele control function in order to be operational for real time information exchange. For this kind of information, a delay increase could be considered as a lost of communication. A guaranteed bandwidth is required only for the purpose of defining the minimum bandwidth required in a MV Secondary substation.
33	Bandwidth allocation	Performance	WP2	SGEC DCAC MVDAC FLIR	Bandwidth ~ 100 kbps	XL	COULD	The delivery of real time information for FLIR, DCAC and SGEC requires the timely exchange of several hundreds of bytes. For MWFM applications with maps require a suitable bandwidth to support the field workers.
34	Packet Loss	Performance	WP2	MVDAC	Packet Loss for MV secondary substations	L	COULD	If packet lost is high Grid Control application becomes not so interactive as designed and safety problems could arise when switching circuit breakers

35	Batteries Autonomy	Performance	WP2	MVDAC FLIR	All ICT elements that provide Tele control function must have a Battery that isolate them from the power supply	XL	COULD	One of the typical operations of MV-DAC from the utility control centre use case is to switch off and switch of an electrical line that feed an area. It is very important that all ICT elements that provide the Tele control Function have batteries with a suitable autonomy in order to not be affected by these typical operations.
36	QoS – networks	QoS	WP2	MVDAC	Every network (or network part) should be able to manage differentiated services through the management of priority levels. Instead of DiffServ e.g. MPLS label switch path protocols can be used.	L	COULD	In case of critical scenarios, when media are shared among multiples parties and network congestion is considered very high, it would be useful to characterize the traffic with at least two priority classes.
37	QoS – applications	QoS	WP2	MVDAC	Relevant applications may be implemented using priority aware libraries.	M	SHOULD	
38	High priority asynchronous messages	QoS	WP2	SGEC	In case of alarms, e.g. in conjunction with power inverters, the according asynchronous messages must be transported very fast to the controller, as alarms normally reflects a very soon loss of energy production. In order to further guarantee the stability of the smart grid, therefore, this information must be transported with highest priority or via reserved communication channels. Without time-synchronization just the priority of the (asynchronous) telegram can be used to reduce the latency from submitting the message until receiving it.	M	MUST	In order to be able to stabilize the grid even in case of big energy losses as a consequence of a failure situation (e.g. within a DER) the controller must be informed immediately about the new situation. The controller then is forced to use such high priority channels in order to redirect energy to maintain stability of the grid.
39	Service discovery mechanism to set appropriate CoS for communication	Service oriented approach	WP2	SGEC DCAC MVDAC FLIR	A service discovery mechanism needs to be specified and implemented in order to set the communication network CoS according to the SG-devices´ communication requirements.	L	MUST	
40	Communications network management	Management	WP2	SGEC DCAC MVDAC FLIR	The devices of the system shall support a network management system (NMS) e.g. SNMP and MIB for network information management. The management system should provide visualization of the status of all network elements for easy overview of the whole network.	L	MUST	Inventory and operational control of the communication network

41	Data management	Management	WP2	SGEC DCAC MVDAC FLIR MWFM	The use case involves handling (processing, analyzing, semantically classifying and accessing) large volumes of data that partially have to be stored for later use (e.g. billing, planning, historical analysis, regulation). The data must be kept consistent and synchronized with other systems within seconds. Data consistency has to be executed by DMS/SCADA system	XL	MUST	
42	Data values checking	Management	WP2	SGEC DCAC MVDAC FLIR MWFM	The use cases involve monitoring and otherwise retrieving large amounts of data from different parts of the distribution network. The data integrity ensures that there is no tampering with the data but still there could be problems e.g. with sensors. Malfunctioning devices of the SG could produce data that should not be accepted by the receiving entity. This can be considered as a certain kind of sanity check, but it can also be utilized with fault detection procedures. This is a requirement for the application level of the SG system software.	XL	MUST	Unacceptable data values must be detected in order to prevent undesirable application behavior and to notify the system of possible malfunctioned equipment.
43	Remote configuration	Management	WP2	SGEC DCAC MVDAC FLIR	The network management system should support remote configuration of the equipment. Remote reset of the devices should be available. Remote SW updates of substation and devices shall be possible.	L	MUST	Lower cost and faster time to equipment's upgrade.
44	Grid operator interface	Usability	WP2	SGEC DCAC MVDAC FLIR MWFM	The display (HMI) of the grid control application to the grid operator has to be clear and intuitive, providing maximum usability, as it may be used in stressing situations. In case of Demand Side Management, the tariff/price information received from the network has to be understandable both by the automatic home/building energy management system and by the customer (person)	M	MUST	

45	Authentication and authorization	Security	WP2	SGEC DCAC MVDAC FLIR MWFM	System components shall uniquely authenticate users and specific components before establishing a connection. The components shall enforce separation of duties through assigned access authorization. The user privileges should be restricted to only those that are required for each person's role, taking into account emergency cases. In situation of emergency user rights override option should be always implemented by providing higher priority than security/access control.	L	MUST	Peer authentication is the first step towards a secure session establishment and thus builds the base for secured communication. Moreover, authentication and role association is the basis to ensure, that only authorized personnel is able to perform certain actions requiring a dedicated role level.
46	Data backup and recovery	Security	WP2	MVDAC	Backups of critical software, applications, and data for all components of the SCADA system should be assured. Backup should be all data and applications needed to replace failed components within a reasonable period of time as required to satisfy regulatory requirements and to restore the system to normal operation. Backups shall be physically separated from the operational components. Synchronization of the backup and operating data must be assured.	XL	MUST	
47	Data confidentiality	Security	WP2	SGEC DCAC MVDAC FLIR MWFM	It shall be possible to ensure the confidentiality of the communicated data by cryptographic mechanisms, unless otherwise protected by alternative physical measurements. The latency introduced from the cryptographic mechanism shall not degrade the functionality of the system.	L	MUST	This requirement relates to the need for confidentiality when information is being transmitted from one entity or a group of entities to another entity or a group of entities as well as locally stored data. The data should be accessible only to authorized users as it is sensitive from a privacy (e.g. user behavior pattern), safety, or economical point of view.

48	Data integrity	Security	WP2	SGEC DCAC MVDAC FLIR MWFM	It shall be possible to ensure the integrity of the communicated data and to verify whether the data hasn't been tampered. The latency introduced from the protection mechanism shall not degrade the functionality of the system.	XL	MUST	Integrity protection when information is being transmitted from one entity or a group of entities to another entity or a group of entities is necessary in order to assure that the data hasn't been altered during transmission. Integrity is needed for the communication of information among SCADA system-RTU-Power equipment, Counter-Measures Hub, or actors like Markets and DSO.
49	Non-repudiation	Security	WP2	SGEC DCAC MVDAC FLIR	It shall be possible to prove that information has been send by a specific source.	L	MUST	
50	Malicious code protection	Security	WP2	SGEC DCAC MVDAC FLIR	The smart grid system shall employ malicious code protection mechanism. The protection mechanisms shall be deployed in such a manner as to limit the impact of the attack to a small geographical area prior to detection and eradication.	M	MUST	One challenge is that the field deployed devices are typically not suitable for traditional third party malicious code protection mechanisms. This combined with very little or no physical security means that emphasis be placed on the risk associated with these widely dispersed assets. Therefore it should be ensured that no malicious code can pass some security zones (e.g. from the utility's NAN to HAN). Field tools represent potentially high risk also because they may be connected to numerous networks.
51	Intrusion detection	Security	WP2	SGEC DCAC MVDAC FLIR	The system shall detect the anomalous events (e.g. meter data alerted) within the network boundaries.	XL	MUST	

52	Denial-of-service protection	Security	WP2	SGEC DCAC MVDAC FLIR	The system should restrict the ability of internal or external users to launch denial-of-service attacks against the network components.	XL	MUST	As single security product or technology cannot protect an energy network control system, a multiple layer strategy involving two or more different overlapping security mechanisms (defense-in-depth), is advised so that the impact of a failure in any one mechanism is minimized. Except for authentication and authorization other access protection means should be used to monitor potential attacks.
53	Cryptographic Key Establishment and Management	Security	WP2	SGEC DCAC MVDAC FLIR	Cryptographic protection and key management infrastructure shall be selected. The selection should match the value of the information being protected and the protected system operating constraints.	XL	MUST	
54	Scalability	Scalability	WP3	All	Scalability is the guarantee that a system can grow without compromising its operations. The Microgrid Control Center cannot be collapsed if its success leads him to grow even more than originally expected.			The Microgrid Control Centre devices should be able to support new remote installations to a number that should never reach.
55	Conformance to standards	Interoperability	WP3	CUC-1.2	Monitoring and control are two basic functionalities of the Microgrid Control Center. The Microgrid Control Center communicates with a large set of different devices from different domains (e.g. from intelligent loads to large wind turbines). To ensure interoperability the communication should rely on well-known and frequently used standards like IEC 61850, IEC 61968/61970 (CIM), or IEC 60870-5-101/104 (Tele control) and others. Also to be respected are specialized communication standards like - IEC 61400-25-4 for wind turbines,- IEC 62270 Hydroelectric power plant automation - Guide for computer-based control, - IEC 62271 Standards for high-voltage switchgear and control gear,- IEC 62325 Standards related to energy market models & communications, IEC 62351 Power System Control and Associated Communications - Data and Communication Security, and others			Open standards is a prerequisite for interoperability

56	MG Controller and management system applicability	Interoperability	WP3	CUC-1	MG Controller and management system should be applicable for wide range of Microgrids. Controller and management system with generic configuration will support several types of microgrid setups.			
57	Mappings between different information models	Interoperability	WP3	CUC-1.2 CUC-1.3	Monitoring and control are two basic functionalities of the Microgrid Control Center. The Microgrid Control Center communicates with a large set of different devices from different domains (e.g. from intelligent loads to large wind turbines). Today a large number of different standards exist and it is very likely that this will also be true in the future. To ensure interoperability between different standards with different information models the standards have to be harmonized. A flexible mapping tool is needed to map monitoring and control data points from different information models onto each other. E.g. the mapping tool should be designed to minimize the manual input and mapping information should be re-usable. An important mapping guideline, for instance, is IEC 61850-80-1 which describes a mapping from IEC 61850 data to IEC 60870-5-101/104. Mapping to IEC 60870-5-101/104 is and will stay a very important task since a large number of legacy devices and systems are only able to run this standard, and switching to other control systems is a big challenge for each system operator which will not be realized very soon.			Not a single standard will cover all relevant points and interoperability can only be ensured by the harmonization and mapping of standards.

58	Data bus	Data management	WP3	CUC-1.2 CUC-1.3 CUC-2.1 CUC-2.2.1 CUC-2.2.2 CUC-2.2.3	Data management is one of the key features of the Microgrid Control Center (MGCC) where high volumes of real-time and historical, static and dynamic operational data are distributed and/or replicated for parallel processing and access. That means up to thousands of data points have to be instantaneously processed, coordinated, manipulated and interpreted if the Microgrid Operator wants to take full advantage of all resources. Following a service oriented architecture the Microgrid Control Center should include a data bus which enables the communication and information exchange between different services in the MGCC. The data bus should provide different communication services (e.g. request/response, publish/subscribe, transactions). Furthermore, it should support different levels of Quality of Service because different applications have different demands, e.g. w.r.t. latency, frequency of data exchange, quality or time synchronization.			The Microgrid's Data Management System classifies, processes, correlates and filters the monitored data, and provides meaningful state information of the Microgrid which in turn can be used by all control and management applications. Transforming and analyzing this data into useful business and operational intelligence is one of the biggest challenges for the Microgrid. For this purpose a flexible service bus supporting Quality of Service is crucial.
59	Database system	Data management	WP3	All and in particular CUC-1.3	Data management including a database system is one of the key features of the Microgrid Control Center (MGCC) where high volumes of real-time and historical, static and dynamic operational data are distributed and/or replicated for parallel processing and access.			E.g., switching network configuration to and from Islanding Mode needs for Optimal Power Flow, to initiate and configure the new context.
60	Self-organization	Automation	WP3	CUC-4	If a system disturbance provokes a general black out such that the microgrid (MG) was not able to separate and continue in islanding mode, and if the system is unable to restore operation in a specified time, a first step in system recovery will be a local black start. The different components of the MG have to self-organize themselves before reconnecting to the grid	M	MUST	
61	Coordination	Automation	WP3	CUC-4	If a system disturbance provokes a general black out such that the Microgrid (MG) was not able to separate and continue in islanding mode, and if the system is unable to restore operation in a specified time, a first step in system recovery will be a local black start. The local controllers of the MG need to dynamically coordinate each other and with the MG control center for the recovery	L	MUST	

62	Distributed Processing	Processing	WP3	CUC-1 BUC-1.1 CUC-4	For balancing supply and demand the Microgrid Control Center has to run the state analysis and define the sub-sequent actions. These tasks include power flow calculations and forecasting models. To minimize processing latency the jobs could be processed in parallel and distributed across different machines. Also for forecasting, planning and revenue in the revenue distributed processing capabilities are crucial.			
63	High Demand for Computing Resources / Processing	Processing	WP3	All	For some use cases, it is necessary to provide high performance computing resources for calculation and simulation models in the Microgrid Control Centre including real-time processing. One example is switching to islanding mode in order to quickly check availability of electrical resources in case islanding of the microgrid is required. Also for long-term planning it may be necessary to provide high performance processing for large-scale planning and simulation. In order to optimize power flow in case of switching to islanding mode, high demand for computing resources for calculation and simulation models in Microgrid Control Centre is required. In order to optimize power flow in case of switching to connected mode, medium processing demand for adaptation to electrical parameters in Overlay Grid is required.			
64	Demand management based on criticality of loads	Processing	WP3	CUC-2.2.1 CUC-2.2.2	MG management and control system shall control loads and enable smart load controlling (cancellation of loads, shifting if loads etc.).			
65	Network Configuration	Auto-configuration	WP3	CUC-5.2 CUC-5.3 CUC-5.4	When new devices (e.g. DER, Network Smart Devices) or sub-systems (e.g. Home/Building Energy Management Systems) are installed in or at the edge of the Microgrid they automatically configure itself (also frequently denoted as Plug & Play). This requirement focuses on IP address configuration and addressability of the device by the Microgrid Control Center.	M	MUST	Network configuration is a prerequisite for all use cases which rely on communication.

66	Device Description	Auto-configuration	WP3	CUC-5.2 CUC-5.3 CUC-5.4	When new devices (e.g. DER, Network Smart Devices) or sub-systems (e.g. Home/Building Energy Management Systems) are installed in or at the edge of the Microgrid they automatically configure itself (also frequently denoted as Plug & Play). This requirement focuses on the description of the capabilities of a device or sub-system	L	MUST	In several Microgrids use cases it is unlikely that a static engineering process is done for the whole system (e.g. supply-side and demand-side management). The Microgrid shows dynamics and the engineering has to be adapted to these circumstances. It has to become an online process supporting the Plug & Play feature for devices.
67	Registration & Look-up	Auto-configuration	WP3	CUC-5.2 CUC-5.3 CUC-5.4	When new devices (e.g. DER, Network Smart Devices) or sub-systems (e.g. Home/Building Energy Management Systems) are installed in or at the edge of the Microgrid they automatically configure itself (also frequently denoted as Plug & Play). This requirement focuses on the registration of the device or sub-system at a registry which is operated e.g. as part of the Microgrid Control Center.	L	MUST	In several Microgrids use cases it is unlikely that a static engineering process is done for the whole system (e.g. supply-side and demand-side management). The Microgrid shows dynamics and the engineering has to be adapted to these circumstances. It has to become an online process supporting the Plug & Play feature for devices.
68	Reliability and Availability (R&A) for the system	Reliability and Availability (R&A)	WP3	All	For all use cases, the reliability and availability of all devices and systems are crucial; this is especially true for the control centre systems. All possible actions and monitoring concepts must be installed to avoid any breakdowns of the systems. The acceptable breakdown/unavailability times may be different for the different systems and may be defined accordingly. It is also required to install fallback or replacement systems that can almost immediately take over crucial actions and processes. If availability and reliability cannot be guaranteed for all the devices the overall system has to be robust w.r.t. disturbances and failures to ensure the stable operation of the Microgrid.	M	MUST	Reliability and availability is one of the crucial ICT requirements.

69	Reliability and Availability (R&A) for the communications	Reliability and Availability (R&A)	WP3	All	For all use cases, the reliability and availability of the communication between the different devices / systems is also crucial; failure in communication (especially concerning control messages) may harm the electrical network to a very deep extent. Failures in electrical devices also must be reported and recognized immediately. Resilience strategies must be planned and ready for taking over communication whenever there is a bottleneck in communications. Strategies and algorithms must be prepared to recognize problems and bottlenecks in communication in time (i.e. before they happen).	M	MUST	Reliability and availability is one of the crucial ICT requirements.
70	Modularity of Hardware Devices	Future proofness	WP3	All	Communication technology is developing rather rapidly. More and more bandwidth will be provided for communication. Wireless reliable secure communication will replace wired communication more and more in the future. It should be easy to replace one communication technology with another one simply by exchanging HW modules at the network devices. Changing or upgrading the physical medium should have no impact on other layers, especially the application-layer.		Optional	Avoids costs for changing communication technology.
71	Modularity of software devices	Future proofness	WP3	All	IT technology is developing rather rapidly. More and more flexible communication and service architectures will be provided. Wireless reliable secure communication will replace wired communication increasingly in the future and Plug & Play will dominate modular designs. It should be easy to replace or extend communication or application service modules by exchanging or adding SW modules. Changing, adding or upgrading services should not cause redesigns.		Optional	Avoids costs for changing communication technology.

72	Publish / Subscribe	Communication services	WP3	BUC-1.1 BUC-2	In asynchronous messaging a system places a message in a message queue based on internal logic or event and does not need to wait for a reply to continue processing. Subscribers express interest in one or more message classes, and only receive messages that are of interest for them.	M	MUST	Business operations will be completed in a non predictable manner, so an asynchronous publish/subscribe service will be mandatory. For most of the control use cases, the messages within the microgrid would be synchronous, however, there may be asynchronous messages, too, in which either the remote location takes the initiative to contact the Control Centre Systems when a predetermined threshold has a been exceeded, or the central point requires a concrete data from a remote location.
73	Request/Response	Communication services	WP3	BUC-1.1 BUC-2	Data will be sent on a request, when a system is asking for certain information and the Data Provider response back to that system with requested information or at least acknowledging the request.	M		Request-response or request-reply is one of the basic methods computerized systems use to talk to each other. When using request-response, the first system requests some data and the second system responds to the request.
74	Time synchronization	Communication services	WP3	BUC-1.1 BUC-2	To achieve network wide synchronization of control tasks on different time-ranges and scalability up to hundreds of systems, while being robust to topology changes and failures, a time-based synchronization method by utilizing concepts of e.g. time-stamping and skew compensation with linear regression is needed.	M		Certain types of control applications require synchronized action sequences, on one hand for stringent and fast aligned control tasks (no jitter) or on the other for completing control tasks under upper limits of time.
75	Latency	QoS	WP3	BUC-2 BUC-3 CUC-1.1 CUC-1.5 CUC-1.6 CUC-2.1 CUC-2.2.1 CUC-2.2.2 CUC-2.2.3 CUC-4	Latency is either one-way delay or round-trip delay. It is always very important to additionally define at which communication layer a latency value should be measured (bit level, TCP packet level, application layer). Values for latencies or delays must reflect the transmission and propagation times that are acceptable for the communication between devices / systems so that information is available in time and possible reactions can be initiated or handled as necessary. The main distinction for latency is:- RT (real-time): delay is deterministic and generally in the range of milliseconds- non-RT: delay is in the range of seconds or more	M	MUST	The Balancing and Ancillary markets (BUC-2) would operate in minutes delay range, so in this case the latency will not be critical. The latency requirement for monitoring and remote control tasks (CUC-1) in conventional electrical networks is about tenths of a second, and so should be for Microgrids. If in the future Microgrids plan to carry out security duties, the maximum tolerated latency would be about a few milliseconds.

76	Bandwidth - Throughput / Good put	QoS	WP3	BUC-2 CUC-1.5 CUC-3.2	Bandwidth is a measurement of maximal possible number of bits or bytes that can be transferred over a communication link (wired or wireless) within 1 sec. respecting all channels served at the same time. Throughput is the real number of bits and bytes that can be transmitted between 2 endpoints of communication within 1 sec., dependent of the number of other communication channels on the same line or medium, the communication environment etc. Good put is the number of packets, bits or bytes that are correctly transmitted to the receiving data endpoint within 1 sec. It is mostly lower than the throughput because retransmission of information may be necessary in bad or disturbed connections.	M		Conventional Monitoring, Metering and Remote control task in electrical are not High Bandwidth demanding, 128 Kbits are more than enough in most cases. Only the main points of the networks, as the control centers demand more bandwidth, but even in this case 2 or 4 Mbits are enough. New standards like IEC 61850 are more bandwidth requesting, but even in this case, the nowadays communications networks are ready to satisfy those requirements. There are different requirements for the different use cases, almost all required medium or low bandwidth. The exact values (i.e. what does low / medium / high bandwidth really mean?) will be defined later.
77	Packet Loss	QoS	WP3	All	Packet loss here means the maximum acceptable percentage of lost packets on a communication link. The lost packets may be retransmitted (reducing the good put) or not. In the latter case the acceptable packet loss rate means the number of lost packets that would allow the receiving endpoint to realize the communication with a quality that may still be acceptable for the user (i.e. in video transmission: with which percentage of lost packets a video transmission may still be reasonable for the user at the receiving end?)	M	MUST	QoS is mandatory in the Telecommunication Network, even if it is a private network.
78	Priority	QoS	WP3	All	Priority in transmission scheduling is an easy way to prefer data of one connection compared to other connections.	M	MUST	The remote control traffic should be prioritized over any other, afterwards the monitoring and metering traffic and finally the traffic dedicated to measurements.
79	Remote control of equipment	Management	WP3	CUC-5.3	The Microgrid Operator needs to remotely control the power electronics of the DER Units in order to provide system services to the overlay grid or to control technical parameters within the Microgrid.			

80	Asset management	Management	WP3	CUC-6	Inventory of equipments, appliances, lines in the microgrid.			
81	Topology view	User Interface	WP3	CUC-6	Visual view of generation and consumption locations (preferable connection with asset management).			
253	Security Services	IT Security	WP3		Security is a very important requirement for the future. To which extent WP3 will handle this topic must still be discussed.		MUST	A high level of security in all the Microgrid Telecommunication Network it´s mandatory. From the point of view of the business, as intelligent meters and other billing systems should never be reached from somebody not authorized and ensure the electrical supply against possible sabotage to the grid. From a control point the Microgrid is a critical infrastructure and has to be protected against accidental and malicious activity.
82	ARQ/FEC	Data Communication	WP4		The data link layer must provide sufficient error detection and/or error correction to enable effective communication. In case of error detection, an ARQ scheme or a implicit failure notice to the user must be implemented	S	MUST	
83	Bandwidth of building access network	Data Communication	WP4	Home #2, #3, #4, #5, #6, #7 RB #1	The connection needs to guarantee the necessary bandwidth so as to send information on the building (identifier), and power and energy information for each one of the appliances that are being monitored and managed. The required bandwidth must be suitable for fixed and mobile communications between the platform and the building gateway.	XS	MUST	The biggest amount of data exchanged between the gateway and the service platform will happen when the customer connects remotely to real time energy monitoring applications.

84	Connectivity : always on	Data Communication	WP4	Home #1, #4, #5, #6, #7, RB #1	There must be an always on connectivity between the service platform and the home gateway, either fixed or mobile. Connectivity between the building gateway equipment and the platform must be 'always on' in the sense that at any time the consumer wants to access the service (through the corresponding applications, no matter the platform), connectivity with the building must be established, to get up to date information on power and energy consumption and to send control commands if requested by the consumer. This requirement could be modulated according to criticity of considered EE services.	M	MUST	Energy efficiency services should run in local equipment in the building to ensure quality and guaranteeing that the service will be provided even in case of network failure.
85	Connectivity : high-level	Data Communication	WP4	All	This requirement relates to the need to “connect” in all relevant senses of the word all devices, appliances, and more generally all physical entities that need to have a network presence inside the extended perimeter of the building management system. Getting this presence means getting connected at all relevant levels, from physical to application level, even in the absence of some of the intervening network protocols. This connectivity includes being part of a relevant device/appliance entity ontology, which corresponds to the highest level of connectivity, i.e. the semantic level.	L	MUST	
86	Latency	Data Communication	WP4		Latency requirements are not critical within the building and can easily be met by all current networking technologies; specific latency requirements arise in the case of separation of the BEMS between a local and a remote part;		COULD	
87	Physical layers	Data Communication	WP4		The physical layers used must allow the coexistence of several communication standards by separation in the frequency, time, coding or spatial domain according to standards	S	MUST	coexistence on the physical layer is a requirement for the coexistence on higher levels-

88	Control commands latency	Data Communications	WP4	Home #4, #5, #7, #8	Control commands from local/remote user interfaces must reach physical appliances with minimum delay (acceptable by the human user). When the consumer connects to the energy efficiency services, either locally or using a remote interface (any application, independently from the platform used: pc, mobile, Smartphone, etc), control commands must be applied in the physical appliance in a time perceived by the consumer as acceptable (bellow 2 seconds)	L	MUST	Consumers must be aware that the controls commands they have demanded over the appliances have get the corresponding answer over the appliances. For that reason a maximum time of response is needed. Otherwise the user would think that the command has not been sent and probably will send it again.
89	Energy Services and applications decoupled from available in-home/building communications technologies	Data Communications	WP4	Home #2, #3, #4, #5, #6, #7, #8, RB #1	Energy services and applications, while enabled through in home/buildings communications, must not depend on one or some specific communication technologies and remain as communication technology agnostic" as possible.	L	MUST	The home environment is heterogeneous with regards to the technologies used by the different home appliances to communicate with the 'central unit' (gateway, energy box). Cabled Ethernet, Wi-Fi, ZigBee, Zwave, PLC based, etc, all of them are competing for the market and up to now and interoperability between technologies at application level is still missing. That is the reasoning while home energy efficiency services logic must be decoupled from the technology used by the appliances to communicate (for monitoring and control).
90	Local processing and storage	Data Processing and Storage	WP4	Optimize Energy Use	Data processing and storage requirements are indispensable for any sort of building-level intelligence and so as to back and inform any communications of building-level software with consumers (through a human-machine interface) or with the grid (through an interoperability interface). See more extended discussion in referenced document.	M	SHOULD	It is obvious that local persistency is required, coupled with redundant cloud-based persistency to support any ICT-heavy energy efficiency mechanisms.
91	Remote processing accumulative values	Data Processing and Storage	WP4	Home #1, #2, RB #1, #2	The platform must offer a way for calculating average consumptions and energy related data and costs: per day, week, month, and year.	XS	MUST	Useful information for the final user

92	Remote processing and storage	Data Processing and Storage	WP4	Optimize Energy Use	The consideration of demand-shaping measures and the implementation of peak shaving capabilities require the grid administrator to have some sort of visibility into the contracts the various loads subscribe to. This is to allow the grid administrator to use a system of compulsory or incentives-oriented measures so as to bring about the intended changes in the load curve. As such, it is necessary to maintain information about the contract model of each subscriber, the options available to that model, and the extent to which some of these options have already been used. Moreover to correctly anticipate future needs both current, real-time, energy demands as well as historical information should be available, on which to base reliable forecasts and ensure the timely initiation of load-shifting measures. Furthermore, and subject to privacy requirements, socio-economic profiles may also need to be available for the various subscribers (even some rough categorization).	M	MUST	
93	Remote processing of comparative values	Data Processing and Storage	WP4	RB #2	The platform should be able to calculate average consumptions and energy related data and costs for buildings with the same profile (homes, depending on the size and use; home buildings; data centers; hotels; SMEs, etc). Average consumptions and costs per day, week, month and year	XS	SHOULD	Useful information for the final user
94	APIs for ESCOs	Interoperability	WP4		The platform (FI-WARE) should offer a standard API for ESCOs so that monitoring and control capabilities available in a building are published for the development of a service. This capabilities need to be qualified with the list of end user roles that can make use of such functionality. For instance, monitoring is not so critical, almost everybody could access these data (taking privacy into account) but control options should be offered only to managers in homes buildings or SMEs.	L	SHOULD	Energy Service providers (ESCOs) need to access to the controllable appliances in order to be able to develop services for final users

95	Common data models (CDM)	Interoperability	WP4	Home #1, #2, #4, #5, #6, #7, RB #1	Definition of common data models (CDM) per type of sensor/appliance. In order to perform energy optimization on behalf of the consumer, home appliances must be modeled in a common way so that the intelligence in the system is able to monitor them, know control capabilities, programming capabilities and have at any moment information on the reachability of the device.	L	MUST	Energy Efficiency Service tries to optimize energy use so that only the minimum energy required is spent to have the desired service. Common Data Models are necessary to offer appliance/sensor manufacturers the minimum set of functionalities that the devices should implement to be used by efficiency services.
96	External Interoperability	Interoperability	WP4	Shape Demand, Shed Electric Loads, Shift Electric Loads	For the purposes of peak shaving, and demand-side management the residential building, on the one hand, and the smart grid, on the other, need to engage in a conversation that's rich in semantic content and could be very heterogeneous in the mechanics and modalities it employs. The object of this "conversation", which can be described as a "protocol" (understood here in a broad sense) is to convey pertinent information and measurements so as to both: (a) enable the grid to communicate to the building a set of rules / imperatives or incentives / counter-incentives, related to demand-side management and, on the other hand to: (b) allow the building to report information, measurements and projections to the grid. See more extended discussion in referenced document.	L	MUST	Advanced features of demand-side management and peak-shaving will be impossible without a well-defined protocol for the building / Smart Grid interface
97	Identification of devices	Interoperability	WP4	Hotel UC #1	The network must allow for unique identification of every device on the network regardless of the physical network it is connected by	M	MUST	Sensor and actuators must be uniquely defined for control actions
98	Internal Interoperability with existing building systems	Interoperability	WP4	OB3 - Optimize Energy Use	Communication layer shall enable interoperation of building management system and other systems existing in the building: access controls, surveillance systems, fire alarm systems.	XL	MUST	Legacy building management systems do not always comprise all the energy-related systems of the building, or any other information systems that may provide data relevant for defining energy strategies, such as building occupancy. Therefore a layer must be built on top of the building that can interface not only a legacy BMS, but also other relevant subsystems of the building

99	Join networks	Interoperability	WP4		The network layer must allow for the combination of two or more separate physical networks into one logical network	M	MUST	This allows managing different site as one network
100	Profiles	Interoperability	WP4	OB3 - Optimize Energy Use	Interoperation with building management systems should allow for definition of personal profiles with different sets of privileges. Concurrent access to data of the different profiles shall be granted	L	SHOULD	Legacy Building Management Systems may not have enough capabilities for defining different profiles which select the information that is shown to different users (i.e. office workers, facility staff, energy service company, security staff, etc.) or the control functionalities that are enabled. Therefore a layer must be built which enables the definition of profiles and the concurrent access of the different profiles to the information retrieved by the BMS
101	Split networks	Interoperability	WP4		The network layer must allow for the possibility to logically split an existing network into several sub networks	M	MUST	In the administration of large networks the logical split may be beneficial
102	Standardization of sensor/appliance monitoring and/or control capabilities	Interoperability	WP4		The devices that are published so that they are available from outside the home should provide a common API (depending on the type) to publish the basic common monitoring and/or control capabilities they offer for service providers. Mechanism should also exist for extended capabilities that some devices could offer beyond these common ones.		SHOULD	Even if in-home sensors are monitored by the home gateway (energy box), there should be a way to make these sensors monitoring and/or control capabilities available from outside the home.
103	Standardization of sensor/appliance eventing capabilities	Interoperability	WP4	Home #3, #6, #8, RB #4	The FI platform should provide the means for home sensors/appliances to send events (triggered by the sensor/appliance itself)	M	SHOULD	This functionality would enable service providers to be notified in case of event (alerts)
104	Standardization of sensor/appliance programming capabilities	Interoperability	WP4	Home #4, #5, #7, #8	The devices that are published so that they are available from outside the home should provide a common API (depending on the type) to publish the programming capabilities they offer for service providers	M	SHOULD	Even if in-home sensors are monitored by the home gateway (energy box), there should be a way to make these sensor programming capabilities available from outside the home.
105	Standardization of sensor/appliance publication protocol	Interoperability	WP4	Home #2, #3, #4, #5, #6, #7, #8, RB #1	There should be provided a mechanism for publishing the sensors that can be remotely monitored in the home. This would enable the use of these sensors by other services different from home energy efficiency services that can manage the information provided in a local manner.	M	SHOULD	Even if in-home sensors are monitored by the home gateway (energy box), there should be a way to make these sensors available from outside the home.

106	Unique building identifier	Interoperability	WP4	RB #1, #2, #3, #4, #5, #6	Each building must have a unique identifier: its geographical location can be used for this if non ambiguous (same building split and under responsibility of several parties) and standard for representation of this location has been agreed on with external parties beforehand	S	MUST	Buildings need to be identified in an unique way
107	Remote alarm management	Interoperability	WP4	OB7 - Check Acute Alerts	User interface shall enable remote alarm visualization and management by multiple operators of the following subsystems: access controls, alarms from thermal/electrical systems, system maintenance alerts, fire detection. All subsystems should be accessible from the same user interface	L	MUST	Critical alerts should reach in real time the appropriate stakeholders and operators (facility managers, energy service companies, etc.) in any location at any time, independently of the Internet connected device that the stakeholder may have available, be it a laptop, a tablet PC or a Smartphone.
108	Enough data storage capacity	Processing and Storage	WP4	RB #1, #2, #6	Requirement will be met without problem, unless old data is never discarded	XS	MUST	Services need to access and manage a huge amount of data for each appliance, in the time and for each building. Adding new buildings quickly is a business requirement for the provision of services
109	Check Energy Use	Reliability & Availability	WP4	OB6 - Check Energy Use	Availability of access to data of current status of the building shall be guaranteed both locally and remotely from Internet connected devices 95% of time	L	MUST	In order to ensure the most critical functionalities derived from other requirements, such as the remote alert management, a very high availability rate of the system must be guaranteed
110	Fall back mode	Reliability & Availability	WP4	Hotel UC #1,5	The system should be able to identify a loss of the communication systems and be able to switch to a fallback mode	M	SHOULD	For safety reasons, it may be beneficial to fall back to a known state, e.g. Turn on the lights

111	Reliability for residential buildings	Reliability and Availability	WP4	Optimize Energy Use	Reliability of the various ICT subsystems deployed at a residential building (these subsystems being used to deliver the various energy efficiency use cases) is critical. The requirement for reliability obviously comprehends not just the hardware but also the software components and not just each one of them separately but also taken together (e.g. reliable coordination and protocols in a distributed setting). However, failures are not life threatening since we are concerned with the reliability of the ICT superstructure and not with the reliability of the underlying energy infrastructure. To that end, architecture should be designed to ensure that latter can survive a breakdown of the former. See more extended discussion in referenced document.	L	SHOULD	Energy efficiency and demand-side management / peak-shaving features require deployment of ICT resources at subscriber's premises. Reliability of said resources is critical.
112	Air conditioning real time control system	Reliability and Availability	WP4	DC1	A real-time monitoring and control of temperatures (which vary with the load of servers) is required to allow significant reliability and availability of the data-center functionalities.	M	MUST	This requirement is mandatory to obtain significant reliability and availability of the data-center functionalities.
113	Free cooling real time control system	Reliability and Availability	WP4	DC2	The use of free cooling system is required to ensure energy saving, reliability and availability at the data-center in case the failures of its air conditioners system	M	MUST	This requirement is mandatory to obtain significant reliability and availability of the data-center functionalities.
114	Power meter usage	Reliability and Availability	WP4	DC3	This ICT requirement allows knowing the difference between the nominal (typically higher) and the one real of the power consumption of the servers in the data-center. So, it is possible increase their number (offering more reliability and availability) without overshooting the power quota allocated.	L	SHOULD	This requirement is recommended because it allows increasing, without impact, the server's number obtaining more reliability and availability.
115	Access based security	Security	WP4	Hotel UC #1	The security concept may use access restriction (based on roles) together with physical location of input devices to implement the role based restrictions of users	M	SHOULD	An identification of the user by every device in the network may not be feasible. It is sufficient to restrict physical access to devices and assume that physical access implies the right to operate the device under a given set of rules.

116	Building Benchmarking	Security	WP4	OB11 - Check Benchmarking in districts	Exchange of data among different office/public buildings shall be implemented in order to enable benchmarking at district or higher levels of buildings of similar characteristics. Data exchange is done in a network external to the buildings, and information provided to each building must not contain sensitive data, e.g. it should be decoupled from the identity of the building.	L	SHOULD	Building benchmarking is one of the main strategies that can be implemented in office and public buildings in order to encourage end users to adopt energy saving behaviors. However, this functionality implies an information exchange among buildings owned by different companies/administrations, which implies a security issue, as it must be guaranteed that no sensitive data is exposed in this information exchange
117	Data Encryption	Security	WP4	OB3 - Optimize Energy Use	Solutions specification shall support data encryption of packets flow with the building systems	M	SHOULD	Data flow coming in and going out of the building must use higher security standards that the data flow within the building, e.g. within a building automation network. Therefore the layer built on top of the systems of the building must incorporate security protocols that protect the data that are sent outside the building
118	Disaster recovery system	Security	WP4	DC4	During primary AC power outage scenarios (due to fortuitous events or to intentional attacks); aggressive power capping can be applied to servers to reduce power consumption. This reduces the power drain on the Uninterrupted Power Supplies (UPSs) increasing the duration the servers can remain operational before on-site generators restore power and cooling.	M	SHOULD	This requirement is recommended because it allows increasing, without impact, the Uninterrupted Power Supplies (UPSs) autonomy in case of blackouts due to fortuitous events or to physical intentional attacks.
119	Role based security	Security	WP4	Hotel UC #1	The security concept must allow for a role based restriction of available actions of users	M	MUST	In order to secure a hotel, only a limited set of actions is available the certain roles, e.g. Guests. This includes e.g. only being able to operate the equipment in the guest's own room

120	Security for residential buildings	Security	WP4	DC4	Use cases discussed in the residential buildings scenarios require the building to store or process information that while not sensitive (e.g. not health or credit-card related), is still personal and access to which by unauthorized parties would be construed as a privacy infringement. See more extended discussion in referenced document.	M	SHOULD	Information whose processing can reveal daily habits or be used to profile a certain electricity subscriber or identify vacancies is stored in various persistent stores at the building and in the cloud. Security of this information and full audit ability of accesses to it should be addressed lest system acceptance is jeopardized.
121	Security for residential buildings	Security	WP4	Engage in Energy-supported Activities of Daily Working	Use cases discussed in the residential buildings scenarios require the building to store or process information that while not sensitive (e.g. not health or credit-card related), is still personal and access to which by unauthorized parties would be construed as a privacy infringement. See more extended discussion in referenced document.	M	SHOULD	Information whose processing can reveal daily habits or be used to profile a certain electricity subscriber or identify vacancies is stored in various persistent stores at the building and in the cloud. Security of this information and full auditability of accesses to it should be addressed lest system acceptance is jeopardized.
122	Workload profiler	Security	WP4	DC5	Develops and executes a series of experiments to characterize how much energy capping can be applied to the servers before the performance target is hit. If implemented, this requirement may increase the autonomy of the UPSs in case of blackouts due to fortuitous events or to physical intentional attacks.	M	COULD	This requirement is recommended because it allows increasing the Uninterrupted Power Supplies (UPSs) autonomy in case of blackouts due to fortuitous events or to physical intentional attacks.
123	Multiple service classes manager	Security / QoS	WP4	#6 Choose between multiple service classes in function of the workloads priority	The high priority workloads run on high security servers; they can take all the power they need to run as fast as they can. Medium priority workloads are assigned to power capped servers. These will run more slowly, but they will still run. The financial manager presents at the customer a tariff that depends from the expected level of the security and quality of services (QoS).	M	SHOULD	This requirement is recommended because it allows to the financial manager to propose at the customer a tariff that depends from the expected level of the security and quality of services (QoS).

124	Direct or emergency load control installation	Self configuration	WP4	SH8 SH10	automatic and secure pairing of control appliances module with the IS of the provider, on one hand, and with smart appliances of the home of another hand		SHOULD	The control system is installed by the provider, not by the customer. So the provider is responsible for the configuration, which should be as simple as possible. A mistake must not be possible, and the system should be protected against a change of configuration allowing either a hacker to take control of the appliances through the control appliance module or directly, or to control the appliances of the neighbors.
125	Display installation & configuration	Self configuration	WP4	Home #1 Home #2 Home #3	automatic and secure pairing of display with meter or meter module, on one hand, and with smart appliances of the home of another hand		MUST	The energy display device is typically connected to the HAN by radio. But the same applies if any other device (PC, mobile, TV,) is used as a display. When installed (e.g. simply powered on, or software installed if PC/mobile based) should not require any complex configuration action from the customer but should only be allowed to link and get the energy consumptions from the meter and the appliances of this home, not of the neighbors.
126	Display installation & configuration	Self configuration	WP4	SH5 SH6 SH7	automatic and secure pairing of display with meter or meter module, on one hand, and with smart appliances of the home of another hand		MUST	The energy display device is typically connected to the HAN by radio. But the same applies if any other device (PC, mobile, TV,) is used as a display. When installed (e.g. simply powered on, or software installed if PC/mobile based) should not require any complex configuration action from the customer but should only be allowed to link and get the energy consumptions from the meter and the appliances of this home, not of the neighbors.
127	easy addition of new server in the energy monitoring tools of the datacenter	Self configuration	WP4	DC3 DC4	It should be easy and require no complex configuration to add a new server to the Intelligent Power Node Manager SW and an Energy Management SW of the Data Center		COULD	

128	easy addition of new wireless sensor to AC control system, of new component to the energy mgt/monitoring system	Self configuration	WP4	DC1 DC2 H3	It should be easy and require no complex configuration to add a new temperature sensor to the sensor network controlling the Air Conditioning of the Data Center. Can be extended to other sensor types for HVAC system, other component of the energy management system		COULD	
129	Energy Management & Optimization System Installation	Self configuration	WP4	SH9 SH11 SH12	Automatic and secure pairing of control appliances module with the meter or the meter module on one hand, and with smart appliances of the home of another hand.		SHOULD	The control system (or HEMS) is installed either by the customer himself, either by a service provider at the request of the customer. The configuration has to be simple and should not allow a hacker or a neighbor to take control of the appliances through the control appliance module or directly.
130	Meter module installation & configuration	Self configuration	WP4	Home #1	automatic and secure pairing of meter module with meter		MUST	The meter module, in the home, is ideally linked by radio or PLC with the meter. When installed (e.g. simply plugged) should not require any configuration action from the customer but should only be allowed to link with the meter of this home, not of the neighbors.
131	Meter module installation & configuration	Self configuration	WP4	SH5	automatic and secure pairing of meter module with meter		MUST	The meter module, in the home, is ideally linked by radio or PLC with the meter. When installed (e.g. simply plugged) should not require any configuration action from the customer but should only be allowed to link with the meter of this home, not of the neighbors.
132	secure and easy connection of office workers to BEMS	Self configuration	WP4	OB9	The office worker should be able to see the DR actions related to him and to its location without complex localization questions. If the worker is given the ability to derogate, this again should be left only to allowed people, based for example on their identity or location, without complex configuration but with enough security to prevent someone to "play" with these facilities.		SHOULD	Hopefully self-explanatory

133	secure connection of BEMS with DR Operator	Self configuration	WP4	OB8 H4 H6	The DR events or dynamic prices must be certified by the originator before being taken into account, so that faked events (or price information) may be dismissed. The verification by the BEMS should require no difficult configuration yet be secure.		MUST	Hopefully self-explanatory
134	Self Configuration general for networked devices	Self configuration	WP4	All	Devices installed by the end consumer without any installer should be plug & play. However shouldn't allow unauthorized access from neighbors, hackers … nor allow the user to hack the neighbors. In installer is mandatory, his skills may not be in ICT but rather in electricity, energy management, etc.	M	COULD	
135	Sensors, appliances etc additional installation and consideration by the BEMS	Self configuration	WP4	OB6 OB7	New sensors, appliances etc should easily join the BEMS in order to report energy consumption to the centralized system or even alarms that could be reported locally or remotely		SHOULD	Any new device consuming energy installed in the building should require no skills to be seen and managed by the BEMS
136	Smart plug additional installation in RB	Self configuration	WP4	RB2	A dweller should easily and securely include a new smart plug in the system and adjust the level of privacy of its information: no diffusion to community, full diffusion to community, restricted (only diffusion of device type but not of the apartment id for example).		SHOULD	As for a social network, the level of detail of information disclosed to the Online Community has to be and remain decided by the dweller
137	Staff connects to the BEMS	Self configuration	WP4	OB6	Facility or security staff should easily connect to the BEMS to get the energy consumption information of the building		SHOULD	The staff is using a non dedicated device (PC, tablet, …) and should easily get connection with the BEMS, after a possible installation procedure on the PC, tablet etc that should be easy and fast (as for current software)
138	Automatic pairing	Self-configuration	WP4	Home #4 Home #6	automatic and secure pairing of control appliances module with the IS of the provider, on one hand, and with smart appliances of the home of another hand		SHOULD	The control system is installed by the provider, not by the customer. So the provider is responsible for the configuration, which should be as simple as possible. A mistake must not be possible, and the system should be protected against a change of configuration allowing either a hacker to take control of the appliances through the control appliance module or directly, or to control the appliances of the neighbors.

139	Service level interfaces having high portability toward the client side	User Interfaces	WP4	DC6	As described DC6, in order to save energy and money, a customer can choose a service that runs workloads having a medium-low dynamic priority. It's natural that the customer wants to monitor the performance/cost ratio for its workload. To do this is required offer service-level interfaces that works properly on the widest possible range of devices, whether they are fixed or mobile, with different operating systems.	M	SHOULD	This requirement is recommended because it's the service that must adapt to the customer devices and not vice versa. Furthermore, it is crucial to offer the customer the perception of the balance between costs and benefits
140	End users interface for Office Buildings	User Interfaces	WP4	OB2 - Control Energy Use Manually	End users of office buildings shall retain control over a limited set of functionalities at local level to some of the systems of the building, without compromising the global energy efficiency strategies set for the whole building. These might include lighting (dimmers, on/off switches), shutter controls, controlled sockets switches, and visualization of energy consumption metering	L	SHOULD	In order to achieve the highest levels of energy efficiency, control strategies of office buildings must be as centralized as possible. Nevertheless, for comfort's sake, some degree of limited control over certain systems can be granted to end users provided that it does not jeopardize the global energy targets set for the building.
141	User feedback	User Interfaces	WP4	Hotel UC #1,5,6	The network must provide a form of user feedback. This can be a return channel in communication or the assured observability of an event by the user	M	MUST	Control actions require feedback. This may be done by using the human to close the control loop, e.g. Light switches, or for slower processes by providing feedback through and HMI. For control loops without human interaction, e.g. Temperature control, the loop must be closed via a return channel.
142	Interoperability of end points for V2G and G2V	ICT Interoperability	WP5	UC-MT-CPA	Syntactic and semantic interoperability between all end points in order to guarantee charge point interoperability	L	MUST	
143	Interoperability of the communication between EVs and Charging Stations	ICT Interoperability	WP5	UC-GO-CLM	Electric Vehicles (EVs) need to exchange data with charge stations, e.g., the current Battery State Of Charge (BSOC) and general technical details such as the maximum charging current. This requires that hardware connections are interoperable and that data exchange protocols and data formats from different EVs can be used at the same charging station.	M	COULD	

144	Interoperability of the communication between EVs and Charging Stations	ICT Interoperability	WP5	UC-VAS-ES	Electric Vehicles (EVs) need to exchange data with charge stations, e.g., the current Battery State Of Charge (BSOC) and general technical details such as the maximum charging current. This requires that hardware connections are interoperable and that data exchange protocols and data formats from different EVs can be used at the same charging station.	M	COULD	
145	Interoperability of Public Charge Points with EV (ICT and Electrical)	Service Delivery	WP5	UC-ST-P	The charging point supports various models of electric vehicles.	L	MUST	
146	Interoperability of Public Charge Points with EV (ICT and Electrical)	Service Delivery	WP5	UC-LT-IRCP	The charging point supports various models of electric vehicles.	L	MUST	
147	Privacy of user data	Data privacy	WP5	UC-ST-H	The information provided (here: location and planned journey) may not be used by other parties	L	COULD	
148	Privacy of user data	Data privacy	WP5	UC-MT-IM	The information provided (here: location and planned journey) may not be used by other parties	L	COULD	
149	Data confidentiality in communication	Security	WP5	All	It shall be possible to ensure the confidentiality of data by cryptographic mechanisms, unless otherwise protected by alternative physical measures. The latency introduced from the cryptographic mechanism shall not degrade the functionality of the system, while the failure of system shall not create denial of service. Data confidentiality here relates to data in transit. This may relate for instance to privacy related data like smart meter information.	L	MUST	This requirement relates to the need for confidentiality when information is being transmitted from one entity or a group of entities to another entity or a group of entities as well as locally stored data. The data should be accessible only to authorized users as it is sensitive from a privacy (e.g. user behavior pattern), safety, or economical point of view.
150	Data confidentiality in databases	Security	WP5	All	It shall be possible to ensure the confidentiality of data by cryptographic mechanisms, unless otherwise protected by alternative physical measures. The latency introduced from the cryptographic mechanism shall not degrade the functionality of the system, while the failure of system shall not create denial of service. Data confidentiality here relates to data at rest, i.e., locally stored data needs to be secured appropriately as well. This may relate for instance to privacy related data like smart meter information.	L	MUST	This requirement relates to the need for confidentiality when information is being transmitted from one entity or a group of entities to another entity or a group of entities as well as locally stored data. The data should be accessible only to authorized users as it is sensitive from a privacy (e.g. user behavior pattern), safety, or economical point of view.
151	Reliability	Reliability	WP5	All	Data transmission has to be reliable	M	COULD	

152	Reliable data transport over heterogeneous networks	Reliability	WP5	UC-MT-IM	Different Communication Service Providers (CSP) is maybe involved in a single data transaction. End-2-End QoS has to be assured over CSP boundaries including identification of Location of Failure.	XL	COULD	
153	Healing mechanisms	Reliability	WP5	UC-MT-CPA	healing mechanisms have to be implemented to keep system in reliable state	XL	COULD	
154	Availability	Availability	WP5	All	All ICT infrastructure has to ensure high availability	L	COULD	
155	Availability of Public Charge Points	Service Availability	WP5	UC-ST-P	Public charge points are available to all as many people as possible.	L	MUST	
156	Availability of Public Charge Points	Service Availability	WP5	UC-LT-IRCP	Public charge points are available to all as many people as possible.	L	MUST	
157	Availability of energy prices	Availability	WP5	UC-GO-CLM	Dynamic energy prices ("Derivation of energy prices") need to be distributed automatically (push) or made available (pull) to charge station providers. In order to facilitate charge station technologies to work with different energy providers, the respective exchange protocols and data formats should be universal.	S	COULD	
158	Availability of grid load information	Availability	WP5	UC-GO-CLM	Dynamic grid load information ("Forecast of grid loads") need to be distributed automatically (push) or made available (pull) to charge station providers. In order to facilitate charge station technologies to work with different grid operators, the respective exchange protocols and data formats should be universal.	S	COULD	
159	Data integrity	Quality of Service	WP5	UC-ST-P	In particular for all payment scenarios, data integrity has to be ensured.	L	COULD	

160	Data integrity	Security	WP5	All	It shall be possible to ensure the integrity of data and to verify whether the data hasn't been tampered with. The latency introduced from the protection mechanism shall not degrade the functionality of the system. Data integrity relates to data in transit and also data at rest, i.e., locally stored data needs to be secured appropriately. This may relate for instance to data like configuration information.	L	MUST	Integrity protection when information is being transmitted from one entity or a group of entities to another entity or a group of entities is necessary in order to assure that the data hasn't been altered during transmission. Integrity is needed for the communication of information among SCADA system-RTU-Power equipment, Counter-Measures Hub, or actors like Markets and DSO. Moreover, local configuration data like access rights or license information needs to be protected too. Firmware updates are another example for protecting data independent of the transport.
161	Low latency of data transmissions for V2G / G2V	Quality of Service	WP5	UC-MT-CPA	The information exchange for grid stabilizing purpose has to be quasi real-time	L	COULD	
162	Low latency of data transmissions for Stored Energy Services	Quality of Service	WP5	UC-GO-SES	The information exchange for grid stabilizing purpose has to be quasi real-time	L	COULD	
163	Remote Upgrade of Infrastructure	Remote accessibility	WP5	UC-ST-P	Required software upgrades of the charging station shall be possible remotely	S	COULD	
164	Remote Upgrade of public charging stations	Remote accessibility	WP5	UC-LT-IRCP	Required software upgrades of the charging station shall be possible remotely	S	COULD	
165	Data management for VAS	System performance	WP5	UC-VAS-ES	High amounts of data have to be stored and evaluated	M	COULD	
166	Data management for V2G / G2V	System performance	WP5	UC-MT-CPA	High amounts of data have to be stored and evaluated in order to allow for grid integration services	M	COULD	
167	Scalable computing resources	System performance	WP5	UC-MT-IM	Computing resources must be highly scalable in order to process data from Inter-modal Services Users and Inter-modal Mobility Operators	L	COULD	
168	Data throughput for ES	System performance	WP5	UC-VAS-ES	High data throughput has to be ensured for all kinds of enhanced Services when high numbers of EV are used	S	COULD	
169	Multi-Communication Media	Modularity / Abstraction	WP5	UC-ST-P	For vehicles that are used in different Use Case categories, different communication media may be required (PLC, Wireless, RFID etc)	M	COULD	

170	Abstraction from Media	Modularity / Abstraction	WP5	All	Despite many different access communication protocols and lots of different hardware solutions, communication must be possible	L	COULD	
171	Data encryption	Security	WP5	UC-ST-P	For all authentication scenarios, the data transmission has to be encrypted	M	COULD	
172	Encryption/Decryption	Security	WP5	UC-MT-CPA	data traffic encryption for sensible personal data	L	COULD	
173	Code and intrusion protection	Security	WP5	All	Limit possibilities of code/data manipulation	L	COULD	
174	Fault detection	Security	WP5	UC-MT-CPA	Faults should be detected as early as possible and communicated to given parties	L	COULD	
175	Secure Network Design	Security	WP5	UC-VAS-ES	The system should restrict the ability of internal or external users to launch denial-of-service attacks against the network components.	XL	MUST	As single security product or technology cannot protect an energy network control system, a multiple layer strategy involving two or more different overlapping security mechanisms (defense-in-depth), is advised so that the impact of a failure in any one mechanism is minimized. Except for authentication and authorization other access protection means should be used to monitor potential attacks.
176	System protection (protection against malicious code, like viruses, intrusion prevention, network access control, etc.) which may be host based or network based	Security	WP5	All	The smart grid system shall employ system protection mechanisms. The protection mechanisms shall be deployed in such a manner as to limit the impact of the attack to a small geographical area prior to detection and eradication.	XL	SHOULD	One challenge is that the field deployed devices are typically not suitable for traditional third party malicious code protection mechanisms. This combined with very little or no physical security means that emphasis should be placed on the risk associated with these widely dispersed assets. Therefore it should be ensured that no malicious code can pass some security zones (e.g. from the utility's NAN to HAN). Field tools represent potentially high risk also because they may be connected to numerous networks.
177	Secure Software/Firmware Updates	Security	WP5	All	The system shall ensure software/firmware updates only with integrity protected packages from an authorized source.	XL	MUST	Malicious software/firmware updates may compromise the whole system.

178	Security Management	Security	WP5	All	Security management has to consider all involved cryptographic protection means, including key management infrastructure, certificate management, security policies, addressing both, technical and organizational means. The selection should match the protection needs of the information being protected and the protected system operating constraints.	L	MUST	
179	Data backup and recovery	Security	WP5	All	Backups of critical software, applications, and data for all components of the SCADA system should be assured. Backup should be applied to all data and applications needed to replace failed components within a reasonable period of time as required to satisfy regulatory requirements and to restore the system to normal operation. Backups shall be physically separated from the operational components. Synchronization of the backup and operating data must be assured.	M	MUST	Backup and (plug & play) recovery is crucial to ensure system availability. This is especially necessary in case of system restarts or replacement of dedicated system parts.
180	Non-repudiation	Security	WP5	UC-MT-IM	It shall be possible to prevent the sender of information from denying sending it.	L	MUST	Authorization validation for audits for dedicated commands. Firmware updates to ensure data origin.
181	Identification of End User in front of Public Charge Points	Identification and Authentication	WP5	UC-ST-P	The user identifies themselves to the energy supplier via the charge point.	L	MUST	
182	Unique Identification	Identification and Authentication	WP5	UC-MT-CPA	Unique Identification per user or car	M	COULD	
183	Identification of End User in front of Public Charge Points	Identification and Authentication	WP5	UC-LT-IRCP	The user identifies themselves to the energy supplier via the charge point.	L	MUST	

184	Authentication and authorization	Security	WP5	UC-LT-A	System components shall uniquely authenticate users and specific components before establishing a connection. The components shall enforce separation of duties through assigned access authorization. The user privileges should be restricted to only those that are required for each person's role, taking into account emergency cases. This reflects least privileged application. Specifically to consider is handling in emergency situations, where a user rights override option should be always implemented. This requires appropriate considerations in the general account policy definition as well as consideration of the specific situation (e.g., by using the situation information (emergency) as additional parameter for access control) This is to (also) address certain types of DoS attacks.	S	MUST	Peer authentication is the first step towards a secure session establishment and thus builds the base for secured communication. Moreover, authentication and role association is the basis to ensure, that only authorized personnel is able to perform certain actions requiring a dedicated role level.
185	Storage of Unique Identity	Identification and Authentication	WP5	LT-1	The EV Users unique identity should be stored on a secure card/fob, secure storage on a phone or secure storage on-board the car, with additional cryptographic material for sharing with other systems	M	SHOULD	
186	Transfer of Unique Identity	Identification and Authentication	WP5	LT-1	The EV Users unique identity should be transferred in a secure way over wireless or wire line technologies	M	SHOULD	
187	EVSE Access Codes	Identification and Authentication	WP5	LT-1	Access codes to EVSE's sent over the medium of SMS / email should be unique	M	SHOULD	
188	Open Web Service APIs of network infrastructure	Protocol/Interface	WP5	UC-VAS-ES	The network infrastructure should feature open web-service API's so that electro mobility cloud services can simultaneously query and reserve both network and cloud services without any human intervention	L	SHOULD	
189	Support of different SLAs of network infrastructure	Quality of Service	WP5	UC-VAS-ES	The network infrastructure should feature numerous levels of SLA's, the best being guaranteed QoS, the worst being best effort QoS.	M	SHOULD	
190	Fully meshed I/O for P2P in network infrastructure	Performance	WP5	UC-VAS-ES	The network infrastructure should feature fully meshed i/o's to support advanced peer-to-peer multimedia service applications	L	SHOULD	
191	Network aggregation nodes	Networking	WP5	UC-MT-CPA	Aggregation nodes are needed in order to use present transport protocols in an efficient way	L	COULD	

192	Provision of Ethernet / IP bandwidth on demand services	Performance	WP5	UC-VAS-ES	the network infrastructure should support the dynamic and random provision of Ethernet / IP bandwidth on demand services so that high definition uni-cast electro-mobility video services can be enabled on demand	M	SHOULD	
193	Real time billing	Management	WP5	UC-VAS-ES	converged energy and communications billing systems should support real time billing	M	SHOULD	
194	Billing mechanism: Mobile or m-Payment	Billing and Payment	WP5	LT-P2	The EVSE should have a way for completing a mobile, m-payment through a CSP		COULD	
195	Billing Mechanism: Access Device	Billing and Payment	WP5	LT-P2	The EVSE access device (card/key fob or mobile) holds details on credit amount available to the EV User		COULD	
196	Billing Mechanism: Top-Up System	Billing and Payment	WP5	LT-P2	The EVSE has a pay as you go system, where the EV User can top their credit on a EVSE Access card		COULD	
197	Micro transactional services	Functional	WP5	UC-VAS-ES	converged energy and communications billing systems should support micro transactional services	M	COULD	
198	Multiple Payment Options at Public Charge Points	Payment	WP5	UC-LT-PM	The charge point provides multiple payment options - cash, card, deferred payment (credited to an account).	L	MUST	
199	Multiple Payment Options at Public Charge Points	Payment	WP5	UC-ST-P	The charge point provides multiple payment options - cash, card, deferred payment (credited to an account).	L	MUST	
200	Wireless and fixed architectures	Performance	WP5	UC-VAS-ES	the network infrastructure should feature a combination of advanced wireless and fixed architectures	S	SHOULD	
201	Wireless coverage	Communication	WP5	UC-MT-CPA	wireless coverage has to be enhanced in order to dynamically receive information on a journey	M	COULD	
202	Wireless entity connection	Communication	WP5	UC-MT-CPA	Cars or users must utilize wireless communication infrastructure since they are moving	S	COULD	
203	Simple Communication EV User - Charge Station	Usability	WP5	UC-GO-CLM	Electric Vehicle Users (EV Users) need to specify preferences such as the Charge Time Frame and the Minimum Battery State Of Charge (BSOC). This can be done in the simplest case by means of a touch screen at the charge station.	XS	COULD	
204	Advanced Communication EV User - Charge Station via Virtualization	Performance	WP5	UC-VAS-ES	The network infrastructure should feature non-blocking advanced virtualization technologies so that many virtual electro-mobility network operators can co-exist on the same physical telecoms network and dynamically scale bandwidth and network services with respect to real-time customer requirements	L	SHOULD	

205	Advanced Communication EV User - Charge Station	Communication	WP5	UC-GO-CLM	Electric Vehicle Users (EV Users) need to specify preferences such as the Charge Time Frame and the Minimum Battery State Of Charge (BSOC). Instead of simple techniques ("Simple Communication EV User - Charge Station"), this could be done more sophisticated and automatically, e.g., with user-friendly agent technology which could be integrated into a navigation system.	M	COULD	
206	In-Car GUI	Performance	WP5	UC-VAS-ES	electro mobility services should be interfaced from an in-car GUI	S	SHOULD	
207	Usability	HMI / GUI / Apps	WP5	All	The user interface has to be simple and self-explanatory	S	COULD	
208	App store	Performance	WP5	UC-VAS-ES	electro mobility application services should be downloaded from a cloud based electro-mobility app store	S	SHOULD	
209	User Context information: EVSE Availability and Tariffs	Information / Data objects	WP5	LT-P1	EVSE Availability and Tariffs can be sent to the EV User	L	COULD	
210	User Context information: Battery Information	Information / Data objects	WP5	LT-P1	EV on-board battery and auxiliary information can be sent to a storage system	M	COULD	
211	User Context information: Geo-Location	Information / Data objects	WP5	LT-P1	An EV Users geo-location information can be sent to a (EV on-board or Online) storage system and can be data mined	L	COULD	
212	User Context information: Profile Information	Information / Data objects	WP5	LT-P1	EV User profile information like preferred Electric Power Supplier and preferred tariff/cost per KM can be sent to a storage system		COULD	
213	EVSE Context Information: Charge Point Availability	Information / Data objects	WP5	LT-P1	The parking bay occupancy status is stored by the EVSE and can be shared with other interested parties		COULD	
214	EVSE Context Information: Tariffs	Information / Data objects	WP5	LT-P1	Up to the minute energy tariff information is available and can be shared with EV Users		COULD	
215	EVSE Context Information: Tariffs	Information / Data objects	WP5	LT-P1	Clear information on EVSE booking fees		COULD	
216	EVSE Context Information: Capabilities	Information / Data objects	WP5	LT-P1	Clear information on EVSE CP capabilities / charging rates (fast charging etc) that can be shared with EV Users		COULD	
217	Environmental Context Information: Weather	Information / Data objects	WP5	LT-P1	3rd Party services can be accessed for weather information		COULD	
218	Environmental Context Information: Traffic	Information / Data objects	WP5	LT-P1	3rd Party services can be accessed for traffic information		COULD	

219	Environmental Context Information: Landscape Topology	Information / Data objects	WP5	LT-P1	3rd Party services can be accessed for landscape/road topology information		COULD	
220	Charge Detailed Record	Information / Data objects	WP5	LT-P2	The format for a Charge Detailed Record has to be defined	S	COULD	
221	Varying Energy suppliers at one Public Charge Point	Service Delivery	WP5	UC-ST-P	Different energy suppliers use the same charging point to deliver their services.	L	MUST	
222	Derivation of energy prices	Charging and Electricity Grid	WP5	UC-GO-CLM	Energy providers need to be able to dynamically derive energy prices for the next hours. This requires precise forecasts of the availability of energy, as well as of the expected demand. Dynamic prices are then a means to balance the energy need and to avoid potentially expensive peaks of the demand.	L	COULD	
223	Forecast of grid loads	Charging and Electricity Grid	WP5	UC-GO-CLM	In electric-vehicle scenarios, unstable electricity grid situations are more likely and they should be avoided. In order to avoid such situations, the grid operators need to be able to precisely forecast the grid load for the next ours. Charge station operators might then react to the current grid situation.	L	COULD	
224	Smart charging scheduling	Charging and Electricity Grid	WP5	UC-GO-CLM	In a smart-charging scenario, a new (near) optimal schedule needs to be calculated whenever certain parameters change.	S	COULD	
225	Logging and Audit	Security	WP5	All	Logging processes shall be established on devices having appropriate resources. Logging supports security monitoring and auditing.	S	MUST	
226	Time Synchronization	Security	WP5	All	Time synchronization keeps timer elements on different components synchronized.	S	SHOULD	Inconsistent timestamps within the overall system restrict monitoring abilities.
227	Access by different connected devices	Service Oriented App.	WP6	WP6_TS_SC1	The contract negotiation should be designed following web-service API, so that different application (including web-based ones) can be developed for different devices.	M	SHOULD	Web-service APIs allow to build final user application for different devices
228	Access by different connected devices	Service Oriented App.	WP6	WP6_TS_SC1	The act of offering energy surplus should be designed by following web-service API, so that different application (including web-based ones) can be developed for different devices.	M	MUST	Web-service APIs allow to build final user application for different devices
229	Access by different connected devices	Service Oriented App.	WP6	WP6_TS_SC1	The act of buying energy surplus should be designed by following web-service API, so that different application (including web-based ones) can be developed for different devices.	M	MUST	Web-service APIs allow to build final user application for different devices

230	Easy-Understable Interface	Usability	WP6	WP6_TS_SC1	The interfaces for all users should be easy-understandable and user-friendly. If not, users would not use the advanced systems.	M	SHOULD	Understandable user interfaces may affect customers involvement
231	Data integrity	Security/Trust	WP6	WP6_TS_SC1	The transmitted and received data about forecasting of energy demand/production have to be reliable	L	MUST	Energy shortage may happen if accurate forecasts doesn't exist
232	Privacy of Contract	Security/Trust	WP6	WP6_TS_SC1	The information provided in contract should not be used by other parties	L	SHOULD	Customers acceptance may rely on a guarantee about confidentiality of own data
233	Data privacy on energy exchange	Security/Trust	WP6	WP6_TS_SC1	The information provided concerning offering energy surplus should not be used by other parties not participating directly in the eMarketplace4E.	L	MUST	Customers acceptance may rely on a guarantee about confidentiality of own data
234	Data privacy on energy exchange	Security/Trust	WP6	WP6_TS_SC1	The information provided concerning buying energy surplus should not be used by other parties not participating directly in the eMarketplace4E.	L	MUST	Customers acceptance may rely on a guarantee about confidentiality of own data
235	Easy-Understable Interface	Usability	WP6	WP6_TS_SC1	The interfaces for all users should be easy-understandable and user-friendly. If not, users would not use the advanced systems.	M	SHOULD	Understandable user interfaces may affect customers involvement
236	Data integrity	Relia/Availability	WP6	WP6_TS_SC1	The data to be transmissed and received have to be reliable in term of truthfulness and timing	L	MUST	
237	Reliability of the system	Relia/Availability	WP6	WP6_TS_SC1	It is very important to guarantee the reliability of the system in term of response time performance	L	SHOULD	Response time and reliability/availability may affect customers involvement
238	Transactional mechanisms	Management	WP6	WP6_TS_SC1	The actions of “offering Energy " and "buying Energy " are meant as ICT transactions between the prosumer and Green Market Operator.	L	MUST	As the most part of eMarketplace in other domains, also the exchange of energy should be performed in a transactional way.
239	Smart Metering	Physical Media	WP6	WP6_TS_SC5	Microgrid Operators need to have Smart Meters and means to analyze/view the corresponding data in order to be precisely aware of e-Island energy consumption/production.	L	MUST	Smart meters need to be available so that e-Island next-to-real-time consumption/production can be monitored
240	Transactional mechanisms	Management	WP6	WP6_TS_SC5	The action of “trading energy” has to be meant as ICT transactions.	L	MUST	This is an essential requirement and the system will not work properly without it.
241	Interoperable and standards protocols for forecasting services	Interoperability	WP6	WP6_TS_SC5	Standard interfaces and protocols have to be used, so that aggregation and forecasting services can be easily integrated. Moreover, different providers have to be able to access the marketplace BT integrating its own system.	M	SHOULD	Different providers are able to easily integrate their own system if standards/protocols exist.

242	Availability/Reliability of forecast in demand/production	Relia/Availability	WP6	WP6_TS_SC5	The Availability of the forecast services have to be high, otherwise energy shortage may happen.	L	SHOULD	Energy shortage may happen if accurate forecasts doesn't exist
243	Microgrid Management Scalability	Scalability	WP6	WP6_TS_SC5	The management of forecast in demand/production of e-Island has to be designed in a scalable way, as it is expected that the amount of users and thus transactions will increase.	L	MUST	High processing demand is needed to fine-grained forecasting at e-Island level. More, the volume of instant data is very high, due the amount of distributed sources.
244	Standardized energy contract	Interoperability	WP6	WP6_IFUCEU_SC4	A standard for energy contracts and energy contract offerings need to be available in order to facilitate trading between all actors and to develop tools such as Web-based electronic marketplaces.	S	SHOULD	Respective standards/interoperability would significantly ease the implementation and acceptance.
245	Marketplace services	Service Oriented App.	WP6	WP6_IFUCEU_SC4	An electronic marketplace needs to be available that facilitates the management, negotiation and closing of energy contracts.	M	MUST	This requirement is essential as the marketplace is the central part of the scenario.
246	Scalability of Marketplace services	Scalability	WP6	WP6_IFUCEU_SC4	The Marketplace Services should be offered in a scalable way, as it is expected that the amount of users and thus transactions will increase.	M	SHOULD	A marketplace makes only sense when it can handle the transactions of all (potential) market participants.
247	Smart Metering	Physical Media	WP6	WP6_IFUCEU_SC4	All consumers need to have Smart Meters and means to analyze/view the corresponding data in order to be precisely aware of their energy consumption.	L	MUST	This requirement is essential as the scenario can only be facilitated with smart meters.
248	Easy-Understable Interface	Usability	WP6	WP6_IFUCEU_SC4	The interfaces for all users should be easy-understandable and user-friendly. If not, users would not use the advanced systems.	M	SHOULD	If the system is hardly usable or unreliable, users will not use the system and the scenario will not work.
249	Data integrity	Relia/Availability	WP6	WP6_IFUCEU_SC4	The transmitted and received data has to be reliable.	L	MUST	This is an essential requirement and the system will not work properly without it.
250	Privacy of Contract	Security/Trust	WP6	WP6_IFUCEU_SC4	The information provided in contracts and offers should not be used by other parties.	L	MUST	This is an essential requirement as nobody would use a system which unnecessarily discloses confidential information.
251	Reliability of the system	Relia/Availability	WP6	WP6_IFUCEU_SC4	It is very important to guarantee the reliability of the system in terms of response time performance, as users would not use the systems otherwise.	L	SHOULD	If the system is hardly usable or unreliable, users will not use the system and the scenario will not work.
252	Authentication and access control	Security/Trust	WP6	WP6_IFUCEU_SC4	All transactions on the marketplace need to be authenticated and the respective users need to have appropriate rights. This requires a role-based access-control system.	S	MUST	This is an essential requirement and the system will not work properly without it.

253	Data management and storage	Performance	WP6	WP6_IFUCEU_SC4	Large amounts of data need to be collected, stored and made available.	S	MUST	This is an essential requirement and the system will not work properly without it.
254	Legally binding electronic contracts	Interoperability	WP6	WP6_IFUCEU_SC4	The legal conditions need to allow to electronically close binding contracts, even if they are closed automatically, e.g., by means of intelligent agents.	M	MUST	When contracts are no legally binding, it makes no sense to trade them electronically.
255	Transactional mechanisms	Management	WP6	WP6_IFUCEU_SC4	Closing contracts should be done giving transactional guarantees.	S	MUST	This is an essential requirement and the system will not work properly without it.
256	Standardized grid issue descriptions	Interoperability	WP6	WP6_TS_SC3	A standard for grid issue descriptions need to be available in order to facilitate automated treatment of such situations, e.g., in an electronic market place.	S	SHOULD	Respective standards/interoperability would significantly ease the implementation and acceptance.
257	Marketplace services	Service Oriented App.	WP6	WP6_TS_SC3	An electronic marketplace needs to be available that facilitates management, collection and selection of grid issues and issue solution (offers).	M	MUST	This requirement is essential as the marketplace is the central part of the scenario.
258	Scalability of Marketplace services	Scalability	WP6	WP6_TS_SC3	The Marketplace Services should be offered in a scalable way, as it is expected that the amount of users and thus transactions will increase.	M	SHOULD	A marketplace makes only sense when it can handle the transactions of all (potential) market participants.
259	Smart Metering	Physical Media	WP6	WP6_TS_SC3	All consumers need to have Smart Meters and means to analyze/view the corresponding data in order to be precisely aware of their energy consumption.	L	MUST	This requirement is essential as the scenario can only be facilitated with smart meters.
260	Data integrity	Relia/Availability	WP6	WP6_TS_SC3	The transmitted and received data has to be reliable.	L	MUST	This is an essential requirement and the system will not work properly without it.
261	Privacy of Contract	Security/Trust	WP6	WP6_TS_SC3	The information provided in contracts and offers should not be used by other parties.	L	MUST	This is an essential requirement as nobody would use a system which unnecessarily discloses confidential information.
262	Reliability of the system	Relia/Availability	WP6	WP6_TS_SC3	It is very important to guarantee the reliability of the system in terms of response time performance, as users would not use the systems otherwise.	L	SHOULD	If the system is hardly usable or unreliable, users will not use the system and the scenario will not work.
263	Transactional mechanisms	Management	WP6	WP6_TS_SC3	Closing contracts should be done giving transactional guarantees.	S	MUST	This is an essential requirement and the system will not work properly without it.
264	Authentication and access control	Security/Trust	WP6	WP6_TS_SC3	All transactions on the marketplace need to be authenticated and the respective users need to have appropriate rights. This requires a role-based access-control system.	S	MUST	This is an essential requirement and the system will not work properly without it.

265	Data management and storage	Performance	WP6	WP6_TS_SC3	Large amounts of data need to be collected, stored and made available.	S	MUST	This is an essential requirement and the system will not work properly without it.
266	Availability	Relia/Availability	WP6	WP6_TS_SC3	The availability of all systems needs to be high in order to be able to solve potentially dangerous grid issues immediately.	S	MUST	This is an essential requirement and the system will not work properly without it.
267	Electricity Network management	Physical Media	WP6	WP6_TS_SC3	Services for monitoring, supervisory control and operation of electrical networks need to be in place.	L	MUST	This is an essential requirement and the system will not work properly without it.
268	Standardized grid issue solution description	Interoperability	WP6	WP6_TS_SC3	A standard for grid issue solutions and grid issue solution offerings needs to be defined in order to facilitate an automated treatment of grid issue situations and to develop tools such as Web-based electronic marketplaces.	S	SHOULD	Respective standards/interoperability would significantly ease the implementation and acceptance.
269	Control mechanisms for Smart Homes	Protocol/Interface	WP6	WP6_TS_SC3	Standardized mechanisms to control the energy consumption and production in Smart Homes from the outside need to be in place. This includes in particular communication interfaces and a protocol for information exchange.	L	MUST	This requirement is essential as the scenario can only be facilitated with such mechanisms.
270	Control mechanisms in the Smart Home	Protocol/Interface	WP6	WP6_TS_SC3	Standardized mechanisms are needed to control of intelligent devices and electric vehicles within a Smart Home (Internet of Things). This includes all aspects: communication interfaces, network connection for all devices and control mechanisms/information exchange (e.g., balancing signals).	L	MUST	This requirement is essential as the scenario can only be facilitated with such mechanisms.
271	Marketplace services	Service Oriented App.	WP6	WP6_TS_SC4	An electronic marketplace needs to be available that facilitates the management, recommendation, negotiation and closing of energy (shifting) contracts as well as notification services and reporting.	M	MUST	This requirement is essential as the marketplace is the central part of the scenario.
272	Scalability of Marketplace services	Scalability	WP6	WP6_TS_SC4	The Marketplace Services should be offered in a scalable way, as it is expected that the amount of users and thus transactions will increase.	M	SHOULD	A marketplace makes only sense when it can handle the transactions of all (potential) market participants.
273	Legally binding electronic contracts	Interoperability	WP6	WP6_TS_SC4	The legal conditions need to allow to electronically close binding contracts, even if they are closed automatically, e.g., by means of intelligent agents.	M	MUST	When contracts are no legally binding, it makes no sense to trade them electronically.
274	Smart Metering	Physical Media	WP6	WP6_TS_SC4	All consumers need to have Smart Meters and means to analyze/view the corresponding data in order to be precisely aware of their energy consumption.	L	MUST	This requirement is essential as the scenario can only be facilitated with smart meters.

275	Easy-Understable Interface	Usability	WP6	WP6_TS_SC4	The interfaces for all users should be easy-understandable and user-friendly. If not, users would not use the advanced systems.	M	SHOULD	If the system is hardly usable or unreliable, users will not use the system and the scenario will not work.
276	Data integrity	Relia/Availability	WP6	WP6_TS_SC4	The transmitted and received data has to be reliable.	L	MUST	This is an essential requirement and the system will not work properly without it.
277	Privacy of Contract	Security/Trust	WP6	WP6_TS_SC4	The information provided in contracts and offers should not be used by other parties.	L	MUST	This is an essential requirement as nobody would use a system which unnecessarily discloses confidential information.
278	Reliability of the system	Relia/Availability	WP6	WP6_TS_SC4	It is very important to guarantee the reliability of the system in terms of response time performance, as users would not use the systems otherwise.	L	SHOULD	If the system is hardly usable or unreliable, users will not use the system and the scenario will not work.
279	Transactional mechanisms	Management	WP6	WP6_TS_SC4	Closing contracts should be done giving transactional guarantees.	S	MUST	This is an essential requirement and the system will not work properly without it.
280	Authentication and access control	Security/Trust	WP6	WP6_TS_SC4	All transactions on the marketplace need to be authenticated and the respective users need to have appropriate rights. This requires a role-based access-control system.	S	MUST	This is an essential requirement and the system will not work properly without it.
281	Data management and storage	Performance	WP6	WP6_TS_SC4	Large amounts of data need to be collected, stored and made available.	S	MUST	This is an essential requirement and the system will not work properly without it.
282	Standardized energy information data	Interoperability	WP6	WP6_TS_SC4	A standard for energy information and analytic results needs to be available in order to facilitate the transactions and additional services offered in marketplace as well as energy information analytics for the smart city.	S	SHOULD	Respective standards/interoperability would significantly ease the implementation and acceptance.
283	Standardized energy contract	Interoperability	WP6	WP6_TS_SC4	A standard for energy (shifting) contracts and energy (shifting) contract offerings need to be available in order to facilitate trading between all actors and to develop tools such as Web-based electronic marketplaces.	S	SHOULD	Respective standards/interoperability would significantly ease the implementation and acceptance.
284	Energy Monitoring	Physical Media	WP6	WP6_TS_SC4	Mechanisms for delivering data related to the energy consumption and/or production within a Smart House need to be in place for planning, procuring and selling activities. Besides Smart Meters, devices need to be intelligent and to be able to communicate.	M	MUST	This requirement is essential as the scenario can only be facilitated with energy monitoring.
285	Forecast of grid load and energy demand	Management	WP6	WP6_TS_SC4	Reliable forecasts of grid load and energy demand are needed for planning generation and consumption.	L	SHOULD	When forecasts are not reliable, the system would hardly work.

286	Rating system	Security/Trust	WP6	WP6_TS_SC4	A rating system is available that facilitates a possibly objective assessment of all marketplace actors. This enables the prosumers to consider them prior to transactions in order to enhance the prosumer's risk management analysis.	M	SHOULD	Without a reliable rating system, the system would hardly work.
287	Info communication system for the Final Users	Service Oriented App.	WP6	WP6_IFUCEU_SC2	A WEB portal that allows to the final user, through a smart phone or a PC, to choose between different energy retailer in order to get at best, technically and economically, its energetic needs.	M	MUST	This requirement is mandatory to obtain Info communication system for the Final Users
288	Cloud computing for high speed data processing	Performance	WP6	WP6_IFUCEU_SC2	To exchange in real time: pricing Information, present demand, available energy to bid and forecast for the future energy demand, a large amounts of data need to be collected and processed in high speed mode through cloud computing.	M	MUST	This is an essential requirement and the system will not work properly without it.
289	Energy Management System	Management	WP6	WP6_IFUCEU_SC2	A metering system installed within the final user home and it will be used to measure energy consumed and/or produced	L	MUST	This requirement is mandatory to measure within the final user the power consumed and/or produced
290	High portability applications for fixed and mobile services targeted to the final customer	Usability	WP6	WP6_IFUCEUSC3	The applications for the services about the eMarket4E have to function properly on the widest possible range of devices, whether they are fixed or mobile, with different operating systems.	L	MUST	This requirement is mandatory because it's the service that must adapt to the customer devices and not vice versa
291	Real time system to monitor the available kind of energy for the energy retailers	Service Oriented App.	WP6	WP6_IFUCEUSC3	A SW WEB-based system that allow to the energy retailers to give the kind of requested energy together at all the necessary market information	L	SHOULD	This requirement is mandatory to monitor in the real time the available kind of energy for the energy retailers
292	A HW/SW network of grid operators to offer different kind of energy	Management	WP6	WP6_IFUCEUSC3	A network of companies that produce different kind of energy and that sell it at the energy retailer.	M	SHOULD	This requirement is mandatory to have different sources of energy for an ethical choice by the end user
293	User Software Agent System	Security/Trust	WP6	WP6_IFUCEUSC3	Autonomous SW entity which observes and stores the final user energy buying habits. Then it acts upon request and directs its activity towards achieving best goals.	L	MUST	This requirement is mandatory because without a network of automata SW is not possible to monitor the habits of end users and make predictions for the immediate future
294	Weather Forecast Service	Service Oriented App.	WP6	WP6_TS_SC2	ICT instrumentation that provides services of Weather Forecast to the Operations Manager or to the Energy Information Provider: this can be very useful for to make forecasts about the energy sources depending from wind, sun etc.	M	MUST	This requirement is mandatory to obtain a very quickly monitoring system to detect rapidly changing phenomena such as wind.

295	Energy information provider	Service Oriented App.	WP6	WP6_TS_ SC2	A WEB based information service dedicated to the very small energy retailers providing them the pricing Information, the present local demand and the available energy to bid. Moreover it performs forecasts for the future energy demand coming from the Facility Manager or the Final Customer.	M	MUST	This requirement is mandatory to ensure the survival of small energy retailers that cannot afford large investments in ICT infrastructure
296	Building data transmission availability	Relia/Availability	WP6	WP6_IFU CEU_SC1	The BEMS installed at the user premises will have to transmit data over the Internet. Always on connectivity and ADSL speeds are required and on the provider side (Marketplace) Data Mining will thus apply.	M	MUST	The Requirement is mandatory to be able to provide the service.
297	Marketplace services	Service Oriented App.	WP6	WP6_IFU CEU_SC1	The service will hold user energy information in detail. And it has to feature the capability of personalizing the interface depending on the context and preferences of the users.	L	MUST	The Requirement is mandatory to be able to provide the service.
298	Data Integrity at the Marketplace	Scalability	WP6	WP6_IFU CEU_SC1	The Information that is to be collected by the Marketplace has to be handled taking care of personalization and context based information.	M	MUST	The Requirement is mandatory to be able to provide the service.
299	Processing capabilities at the Marketplace	Service Oriented App.	WP6	WP6_ IFUCEU _SC5	The Service at the marketplace will have to implement complex operations between the data that will be collected from the Grid users and operators	L	MUST	The Requirement is mandatory to be able to provide the service.
300	Efficient and secure service access and provision	Protocol/Interface	WP6	WP6_ DSM _SC1	The Ability of generating contracts on the fly over the internet will need to be reliable by employing standard protocols and interfaces for the users. Security access has to be provided also following usual	L	SHOULD	The Requirement is mandatory to be able to provide the service.
301	Reliable and deterministic signal commands from the Marketplace	Performance	WP6	WP6_ DSM _SC1	This UC will need reliable and provisioning QoS, since signaling is involved between the GRID and the user BEMS. The latter signals will have to arrive reliably in order to shape the demand curve.	M	MUST	The Requirement is mandatory to be able to provide the service.
302	Real Time Data and Service management	Management	WP6	WP6_ DSM _SC1	The requirement takes on board the fact that in the future real time tariff schemes will have to be handled by the Market place service.	L	SHOULD	The Requirement is mandatory to be able to provide the service.
303	Decision Making and signaling energy commands	Service Oriented App.	WP6	WP6_ DSM _SC1	The service that may lie on the Grid User side or in the cloud needs to know the user contract and the installed capabilities. According to the latter processing capabilities are key to decide how to signal the shape demand commends.	L	MUST	The Requirement is mandatory to be able to provide the service.
304	IPV6 a must for IOT (Customer BEMS and related devices)	Scalability	WP6	WP6_IFU CEU_SC1	The BEMS would have to be uniquely identified at the customer premises and in some cases the devices included in energy efficiency services.	S	MUST	IP addressing shortage

305	Number of customers in the eMarket4E services may grow exponentially	Scalability	WP6	WP6_IFUCEU_SC1	The scenario takes into account the customers that may connect to the service. The latter may raise exponentially and thus appropriate data mining data bases must be taken into account. The numbers may rise easily to the hundred thousand.	S	MUST	In this type of services customers in the professional and residential sectors are considered. Therefore the number of users will rise rapidly.
306	The Emarket4Eservices availability in a year's time	Relia/Availability	WP6	WP6_ DSM _SC1	Depending on the scenario there will be more stringent requirements towards availability of the eMarket4E services. DSM will need an availability % of at least 99%.	L	MUST	IN order to effectively shape the load curve and flatten the demand curve for example, the system should be available every day and failure times should be reduced at the maximum.
307	Speed of communication to the eMarket4E services	Performance	WP6	WP6_IFUCEU_SC1	eMarket4E services will require SOTA internet connectivity speeds. In this case speeds starting at 800 Kbps should be provided.	S	MUST	The services will have to be accessible following standard internet quality levels with a minimum speed in order to ensure user acceptance.
308	Service Transparency at the customer premises: Data Access	Performance	WP6	WP6_ DSM _SC1	Emarket4E services will have to access information coming from various devices at the customer premises. Thus Layer 3 protocols should be supported, Access technology agnostic, compatibility with AAA services and also information appliance agnostic.	M	MUST	The Customer premises systems should be accessible by the eMaket4E services. Thus the protocols and services for AAA should be supported. SOTA data access levels should be supported.
309	Ease of use of the eMarket4E services	Usability	WP6	WP6_IFUCEU_SC1	The services that will be provided at the eMarket4E will have to comply with: Ease of learning, memorability, maintainability, natural interaction and user satisfaction. This refers to the service interaction design in one side (service provider) and on the other by the artifacts provided at the platform side to mash up and produce services.	L	MUST	At the eMarket4E framework, customers are importantly targeted and therefore usability/ease of use should be one of the most crucial requirements to be addressed.
310	Flexibility in the creation of new services interfaces/interaction framework	Usability	WP6	WP6_IFUCEU_SC1	Diverse preferences and abilities of the customers should be taken into account when designing the service interaction of eMarket4E services.	L	MUST	Final customer's acceptance is key and thus flexibility in the user access interfaces should be provided.
311	Self-configuration for non-networked appliances and physical entities	Self-configuration	WP6	All	Devices and appliances that are monitored and possibly controlled by way of external sensors and actuators (e.g. a smart plug) should be recognized and configured in way similar to networked devices with zero-conf plug and play mechanisms	XL	MUST	

312	Monitoring and control user interfaces for building end-users	User interfaces	WP6	All	User Interfaces for building end-users have to be proposed in at least two different ways: as fixed interfaces inside the building, possibly using a dedicated interface devices (like a home/building control panel), and as either mobile or generic remote interfaces. This duality makes it almost mandatory that the support of these interfaces be available outside of the home network, which will also make it easier for third parties to have access to their own user interfaces		MUST	
313	Monitoring, control and management user interfaces for technical staff, facilities managers, etc	User Interfaces	WP6	All	Similar to interfaces for building inhabitants, and excluding the case of homes, these do generally have to be available through fixed or dedicated devices inside the building, and, possibly with reduced functionality, as interfaces outside the building. Similar arguments apply to the support of these interfaces outside the building network.		COULD	

10. Annex III - ICT Requirement to the Architecture Board

FI-WARE Back-log

10.1 Service/Function Layer

Field	ENUM	Description
ID	No	9.EPIC.FINSENY.Service/Function.Reliability
Name	No	Reliability
Goal	No	Guarantee the reliability of the system in terms of response time performance.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Workload characterization should exist in order to perform capacity planning studies to ensure desired performance. Different Communication Service Providers (CSP) are maybe involved in a single data transaction. End-2-End QoS has to be assured over CSP boundaries including identification of Location of Failure. The system should be able to identify a loss of the communication systems and be able to switch to a fallback mode. Application plasticity will be very helpful especially during crisis situation in order to be able to send data to the field workers. Application plasticity will be very helpful especially during crisis situation in order to be able to send data to the field workers. From the Dispatch System point of view, the communication system must be able to "push" data to the worker handset whatever the telecommunication medium the worker is currently using, even if its IP address has changed. Insuring reliability and defining a suitable availability of CT operations towards Aggregator, VPP or DSO processes, applications, databases and the SG-devices.
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Guarantee the reliability of the system in terms of response time performance.
Rationale	No	If the system is hardly usable or unreliable, users will not use the system and the scenario will not work. In order to ensure the most critical functionalities derived from other requirements, such as the remote alert management, a very high availability rate of the system must be guaranteed. For safety reasons, it may be beneficial to fall back to a known state, eg. Turn on the lights. Multihoming with automatic handover management will enhance the possibility for a worker to have access to central data, especially in a crisis situation. Defining availability figures on CT layer is relevant for ongoing operation and also related to safe grid operation. IP mobility is an issue that must be handled by the communication system
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger

Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Field	ENUM	Description
ID	No	16.EPIC.FINSENY.Service/Function.Availability
Name	No	Availability
Goal	No	All ICT infrastructure has to ensure high availability
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	The Availability of the forecast services have to be high, otherwise energy shortage may happen. Dynamic energy prices and grid load information need to be distributed automatically (push) or made available (pull) to charge station providers. In order to facilitate charge station technologies to work with different energy providers, the respective exchange protocols and data formats should be universal. It should be assured (to the most possible extend) that if a component fails, it fails in a manner that does not impact other parts, nor generate unnecessary traffic on the ICS, nor cause another problem elsewhere, such as a cascading event, which would affect other parts and functions. If that cannot be assured a backup/redundancy for the component has to be provided.
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	All ICT infrastructure has to ensure high availability
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	05/08/2011
Last modified	No	05/08/2011

Field	ENUM	Description
ID	No	22.EPIC.FINSENY.Service/Function.Future-proof system design requirements
Name	No	Future-proof system design requirements
Goal	No	Future-proof system design wrt to modularity, standardization, maintainability and HW/SW upgradeability
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Future-proof system design requires modularity, maintainability, upgradeability of hardware, firmware and software as well as long time sourcing
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Future-proof system design wrt to modularity, standardization, maintainability and HW/SW upgradeability
Rationale	No	Functional architecture may become dependent on practically available equipment which is compliant to operational conditions
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	11/07/2011
Last modified	No	11/07/2011

Field	ENUM	Description
ID	No	23.EPIC.FINSENY.Service/Function.Persistent data storage
Name	No	Persistent data storage
Goal	No	SG devices must contain enough non-volatile memory (e.g. flash memory) for storing measurements, internal data, and enable future firmware and software updates.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Configuration Security
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	SG devices must contain enough non-volatile memory (e.g. flash memory) for storing measurements, internal data, and enable future firmware and software updates.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	08/06/2011
Last modified	No	08/06/2011

Field	ENUM	Description
ID	No	24.EPIC.FINSENY.Service/Function.Environmental Requirements for Information and Communication Technology
Name	No	Environmental Requirements for Information and Communication Technology
Goal	No	Communication equipment for SG-field-devices / Field Mobile Devices and IT (Servers) operated reliably under different environmental conditions.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	SG-related communication and control equipment needs to be designed for: - Harsh climate (temperature, humidity) - ESD, RFI, and EMI Immunity (RFI from strong electrical or magnetic fields, EMI related to direct or indirect ESD protection) Operating Environment e.g. based on IEEE 1613 (Sub-Stations) and ETSI EN 300 019 (Telco-Environment)
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Communication equipment for SG-field-devices / Field Mobile Devices and IT (Servers) operated reliably under different environmental conditions.
Rationale	No	Functional architecture may become dependent on practically available equipment which is compliant to required operational conditions
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	11/07/2011
Last modified	No	11/07/2011

Field	ENUM	Description
ID	No	36.EPIC.FINSENY.Service/Function.Quality of Service
Name	No	Quality of Service
Goal	No	Every network (or network part) should be able to manage differentiated services through the management of priority levels.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Application libraries
Status	Yes	
MoSCoW priority	Yes	SHOULD
Relative priority	No	SHOULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Every network (or network part) should be able to manage differentiated services through the management of priority levels.
Rationale	No	In case of critical scenarios, when media are shared among multiples parties and network congestion is considered very high, it would be useful to characterize the traffic with at least two priority classes.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	13/06/2011
Last modified	No	13/06/2011

Field	ENUM	Description
ID	No	38.EPIC.FINSENY.Service/Function.High priority asynchronous messages
Name	No	High priority asynchronous messages
Goal	No	In case of alarms, e.g. in conjunction with power inverters, the according asynchronous messages must be transported very fast to the controller, as alarms normally reflects a very soon loss of energy production. In order to further guarantee the stability of the smart grid, therefore, this information must be transported with highest priority or via reserved communication channels. Without time-synchronization just the priority of the (asynchronous) telegram can be used to reduce the latency from submitting the message until receiving it.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Establish prioritized communication channels Fast priority routing mechanisms Security Means Interoperability of the IT-System on North-bound IT I/Fs. (Wrt processes, applications and databases in the sense of CIM/IEC61968, GID/IEC61970, GIS and Interactions) founded on available standards and extensions. Interoperability on standardized South-bound IT I/Fs as IEC61850, IEC60870, DNP3 used for control and alarm purposes of SG-devices, DER, DG, Storage and SGEC devices.
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	In case of alarms, e.g. in conjunction with power inverters, the according asynchronous messages must be transported very fast to the controller, as alarms normally reflects a very soon loss of energy production. In order to further guarantee the stability of the smart grid, therefore, this information must be transported with highest priority or via reserved communication channels. Without time-synchronization just the priority of the (asynchronous) telegram can be used to reduce the latency from submitting the message until receiving it.
Rationale	No	In order to be able to stabilize the grid even in case of big energy losses as a consequence of a failure situation (e.g. within an DER) the controller must be informed immediately about the new situation. The controller then is forced to use such high priority channels in order to redirect energy to maintain stability of the grid.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	24/06/2011
Last modified	No	24/06/2011

Field	ENUM	Description
ID	No	39.EPIC.FINSENY.Service/Function.Service discovery mechanism to set appropriate CoS for communication
Name	No	Service discovery mechanism to set appropriate CoS for communication
Goal	No	Automatic and secure pairing of display with meter or meter module, on one hand, and with smart appliances of the home of another hand
Version	No	A service discovery mechanism needs to be specified and implemented in order to set the communication network CoS according to the SG-devices´ communication requirements.
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Configuration Security
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Automatic and secure pairing of display with meter or meter module, on one hand, and with smart appliances of the home of another hand
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	08/06/2011
Last modified	No	08/06/2011

Field	ENUM	Description
ID	No	70.EPIC.FINSENY.Service/Function.Modularity of Communication Devices
Name	No	Modularity of Communication Devices
Goal	No	Communication technology is developing rather rapidly. More and more bandwidth will be provided for communication. Wireless reliable secure communication will replace wired communication more and more in the future. It should be easy to replace one communication technology with another one simply by exchanging HW and / or SW modules at the network devices. Furthermore, changing the physical medium should have no impact on other layers, especially the application-layer.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Robustness
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Communication technology is developing rather rapidly. More and more bandwidth will be provided for communication. Wireless reliable secure communication will replace wired communication more and more in the future. It should be easy to replace one communication technology with another one simply by exchanging HW and / or SW modules at the network devices. Furthermore, changing the physical medium should have no impact on other layers, especially the application-layer.
Rationale	No	Avoids costs for changing communication technology.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	05/08/2011
Last modified	No	05/08/2011

Field	ENUM	Description
ID	No	80.EPIC.FINSENY.Service/Function.Topology view
Name	No	Topology view
Goal	No	Visual view of generation and consumption locations (preferable connection with asset management).
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Visual view of generation and consumption locations (preferable connection with asset management).
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Field	ENUM	Description
ID	No	124.EPIC.FINSENY.Service/Function.Direct or emergency load control installation
Name	No	Direct or emergency load control installation
Goal	No	Automatic and secure pairing of control appliances module with the IS of the provider, on one hand, and with smart appliances of the home of another hand
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Configuration Security
Status	Yes	
MoSCoW priority	Yes	SHOULD
Relative priority	No	SHOULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Automatic and secure pairing of control appliances module with the IS of the provider, on one hand, and with smart appliances of the home of another hand
Rationale	No	The control system is installed by the provider, not by the customer. So the provider is responsible for the configuration, which should be as simple as possible. A mistake must not be possible, and the system should be protected against a change of configuration allowing either a hacker to take control of the appliances through the control appliance module or directly, or to control the appliances of the neighbours.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	18/09/2011
Last modified	No	18/09/2011

Field	ENUM	Description
ID	No	125.EPIC.FINSENY.Service/Function.Display installation & configuration
Name	No	Display installation & configuration
Goal	No	Automatic and secure pairing of display with meter or meter module, on one hand, and with smart appliances of the home of another hand
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Configuration Security
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Automatic and secure pairing of display with meter or meter module, on one hand, and with smart appliances of the home of another hand
Rationale	No	The energy display device is typically connected to the HAN by radio. But the same applies if any other device (PC, mobile, TV ...) is used as a display. When installed (e.g. simply powered on, or software installed if PC/mobile based) should not require any complex configuration action from the customer but should only be allowed to link and get the energy consumptions from the meter and the appliances of this home, not of the neighbours.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	18/09/2011
Last modified	No	18/09/2011

Field	ENUM	Description
ID	No	127.EPIC.FINSENY.Service/Function.Self Configuration for Devices
Name	No	Self Configuration for Devices
Goal	No	Any new device that connects to the network must be able to be configured automatically.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	It should be easy and require no complex configuration to add a new server to the Intelligent Power Node Manager SW and an Energy Management SW of the Data Centre It should be easy and require no complex configuration to add a new temperature sensor to the sensor network controlling the Air Conditioning of the Data Centre. Can be extended to other sensor types for HVAC system, other component of the energy management system New sensors, appliances etc should easily join the BEMS in order to report energy consumption to the centralized system or even alarms that could be reported locally or remotely A dweller should easily and securely include a new smart plug in the system and adjust the level of privacy of its information : no diffusion to community, full diffusion to community, restricted (only diffusion of device type but not of the apartment id for example). Devices and appliances that are monitored and possibly controlled by way of external sensors and actuators (eg a smart plug) should be recognized and configured ina way similar to networked devices with zero-conf plug and play mechanisms Identification of appliances and non-networked entities with non models, evn on an approximate basis, process may be iterative and incremental
Status	Yes	
MoSCoW priority	Yes	SHOULD
Relative priority	No	SHOULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Any new device that connects to the network must be able to be configured automatically.
Rationale	No	The control system (or HEMS) is installed either by the customer himself, either by a service provider at the request of the customer. The configuration has to be simple and should not allow a hacker or a neighbour to take control of the appliances through the control appliance module or directly. The meter module, in the home, is ideally linked by radio or PLC with the meter. When installed (eg simply plugged) should not require any configuration action from the customer but should only be allowed to link with the meter of this home, not of the neighbours. Any new device consuming energy installed in the building should require no skills to be seen and managed by the BEMS As for a social network, the level of detail of information discloses to the Online Community has to be and remain decided by the dweller
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	20/09/2011
Last modified	No	20/09/2011

Field	ENUM	Description
ID	No	129.EPIC.FINSENY.Service/Function.Energy Management & Optimization System Installation
Name	No	Energy Management & Optimization System Installation
Goal	No	automatic and secure pairing of control appliances module with the meter or the meter module on one hand, and with smart appliances of the home of another hand.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Configuration Security
Status	Yes	
MoSCoW priority	Yes	SHOULD
Relative priority	No	SHOULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	automatic and secure pairing of control appliances module with the meter or the meter module on one hand, and with smart appliances of the home of another hand.
Rationale	No	The control system (or HEMS) is installed either by the customer himself, either by a service provider at the request of the customer. The configuration has to be simple and should not allow a hacker or a neighbour to take control of the appliances through the control appliance module or directly.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	18/09/2011
Last modified	No	18/09/2011

Field	ENUM	Description
ID	No	133.EPIC.FINSENY.Service/Function.Secure connection of BEMS with DR Operator
Name	No	Secure connection of BEMS with DR Operator
Goal	No	The DR events or dynamic prices must be certified by the originator before being taken into account, so that faked events (or price information) may be dismissed. The verification by the BEMS should require no difficult configuration yet be secure.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Security
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The DR events or dynamic prices must be certified by the originator before being taken into account, so that faked events (or price information) may be dismissed. The verification by the BEMS should require no difficult configuration yet be secure.
Rationale	No	Hopefully self-explanatory
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	18/09/2011
Last modified	No	18/09/2011

Field	ENUM	Description
ID	No	137.EPIC.FINSENY.Service/Function.Staff connects to the BEMS
Name	No	Staff connects to the BEMS
Goal	No	Facility or security staff should easily connect to the BEMS to get the energy consumption information of the building
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Configuration
Status	Yes	
MoSCoW priority	Yes	SHOULD
Relative priority	No	SHOULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Facility or security staff should easily connect to the BEMS to get the energy consumption information of the building
Rationale	No	The staff is using a non dedicated device (PC, tablet, …) and should easily get connection with the BEMS, after a possible installation procedure on the PC, tablet etc that should be easy and fast (as for current software)
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	18/09/2011
Last modified	No	18/09/2011

Field	ENUM	Description
ID	No	138.EPIC.FINSENY.Service/Function.Automatic pairing
Name	No	Automatic pairing
Goal	No	automatic and secure pairing of control appliances module with the IS of the provider, on one hand, and with smart appliances of the home of another hand
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Configuration Security
Status	Yes	
MoSCoW priority	Yes	SHOULD
Relative priority	No	SHOULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	automatic and secure pairing of control appliances module with the IS of the provider, on one hand, and with smart appliances of the home of another hand
Rationale	No	The control system is installed by the provider, not by the customer. So the provider is responsible for the configuration, which should be as simple as possible. A mistake must not be possible, and the system should be protected against a change of configuration allowing either a hacker to take control of the appliances through the control appliance module or directly, or to control the appliances of the neighbours.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	18/09/2011
Last modified	No	18/09/2011

Field	ENUM	Description
ID	No	139.EPIC.FINSENY.Service/Function. Service level interfaces having high portability toward the client side
Name	No	Service level interfaces having high portability toward the client side
Goal	No	As described DC6, in order to save energy and money, a customer can choose a service that runs workloads having a medium-low dynamic priority. It's natural that the customer wants to monitor the performance/cost ratio for its workload. To do this is required offer service-level interfaces that works properly on the widest possible range of devices, whether they are fixed or mobile, with different operating systems.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	This requirement is mandatory because the type of devices used by end users is quite varied: it's the service that must adapt to the customer and not vice versa
Status	Yes	
MoSCoW priority	Yes	SHOULD
Relative priority	No	SHOULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	As described DC6, in order to save energy and money, a customer can choose a service that runs workloads having a medium-low dynamic priority. It's natural that the customer wants to monitor the performance/cost ratio for its workload. To do this is required offer service-level interfaces that works properly on the widest possible range of devices, whether they are fixed or mobile, with different operating systems.
Rationale	No	This requirement is recommended because it's the service that must adapt to the customer devices and not vice versa. Furthermore, it is crucial to offer the customer the perception of the balance between costs and benefits
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	20/09/2011
Last modified	No	20/09/2011

Field	ENUM	Description
ID	No	140.EPIC.FINSENY.Service/Function.End users interface for Office Buildings
Name	No	End users interface for Office Buildings
Goal	No	End users of office buildings shall retain control over a limited set of functionalities at local level to some of the systems of the building, without compromising the global energy efficiency strategies set for the whole building. These might include lighting (dimmers, on/off switches), shutter controls, controlled sockets switches, and visualization of energy consumption metering
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Usability
Status	Yes	
MoSCoW priority	Yes	SHOULD
Relative priority	No	SHOULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	End users of office buildings shall retain control over a limited set of functionalities at local level to some of the systems of the building, without compromising the global energy efficiency strategies set for the whole building. These might include lighting (dimmers, on/off switches), shutter controls, controlled sockets switches, and visualization of energy consumption metering
Rationale	No	In order to achieve the highest levels of energy efficiency, control strategies of office buildings must be as centralized as possible. Nevertheless, for comfort's sake, some degree of limited control over certain systems can be granted to end users provided that it does not jeopardize the global energy targets set for the building.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	21/09/2011
Last modified	No	21/09/2011

Field	ENUM	Description
ID	No	141.EPIC.FINSENY.Service/Function.User feedback
Name	No	User feedback
Goal	No	The network must provide a form of user feedback. This can be a return channel in communication or the assured observation of an event by the user
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Feed back
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The network must provide a form of user feedback. This can be a return channel in communication or the assured observation of an event by the user
Rationale	No	Control actions require feedback. This may be done by using the human to close the control loop, e.g. Light switches, or for slower processes by providing feedback through and HMI. For control loops without human interaction, e.g. Temperature control, the loop must be closed via a return channel.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	18/09/2011
Last modified	No	18/09/2011

Field	ENUM	Description
ID	No	142.EPIC.FINSENY.Service/Function.ICT Interoperability
Name	No	ICT Interoperability
Goal	No	Syntactic and semantic ICT interoperability between all elements of the Grid (HW & SW)
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Interoperability on Communication Technology (CT) layer requires utilization of any useful link available under disturbed operating conditions. Central Dispatch System (CSD) and especially Field Mobile Devices (FMD) systems need to support different physical access paths to establish a connection to the CSD´s gateways. These communication links may be utilized: - LTE/4G and UMTS/3G (e.g. for regular operation), - 2G/GPRS – low speed, - Wi-Fi Internet access via Hotspots, - Satellite Links via public or privately operated networks - Direct Ethernet to connect into public networks - Direct Ethernet to connect into substation networks - DSL (ADSL) modem connection to public operators via twisted pairs (assuming no local power, but central office DSLAM power back-up) - Powerline communications (PLC/BPL to Low Voltage data networks, i.e. into Smart Meter Field Area Communication networks - FAN) - Local Mesh Radio communications (ZigBee, Z-Wave, i.e. into Smart Meter Field Area Communication networks - FAN)
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Syntactic and semantic ICT interoperability between all elements of the Grid (HW & SW)
Rationale	No	Interoperability on CT layer is relevant for a standardized operation and data exchange of related information.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	01/04/2011
Last modified	No	01/04/2011

Field	ENUM	Description
ID	No	145.EPIC.FINSENY.Service/Function.Interoperability of Public Charge Points with EV (ICT and Electrical)
Name	No	Interoperability of Public Charge Points with EV (ICT and Electrical)
Goal	No	The charging point supports various models of electric vehicles.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	The charging point must supports various models of electric vehicles or a standard connector must be developed and used on al EVs.
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The charging point supports various models of electric vehicles.
Rationale	No	If he charging point are not standard to any EV model, the final user must be sure regarding the availability of charging point for his/her model.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	09/06/2011
Last modified	No	09/06/2011

Field	ENUM	Description
ID	No	155.EPIC.FINSENY.Service/Function.Availability of Public Charge Points
Name	No	Availability of Public Charge Points
Goal	No	Public charge points are available to all as many people as possible.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Accessibility
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Public charge points are available to all as many people as possible.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	09/06/2011
Last modified	No	09/06/2011

Field	ENUM	Description
ID	No	162.EPIC.FINSENY.Service/Function.Low latency of data transmissions
Name	No	Low latency of data transmissions
Goal	No	The information exchange for grid stabilizing purpose has to be quasi real-time
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Performance, Usability, Robustness
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The information exchange for grid stabilizing purpose has to be quasi real-time
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/08/2011
Last modified	No	22/08/2011

Field	ENUM	Description
ID	No	169.EPIC.FINSENY.Service/Function.Multi-Communication Media
Name	No	Multi-Communication Media
Goal	No	For vehicles that are used in different Use Case categories, different communication media may be required (PLC, Wireless, RFID etc)
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Configuration
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	For vehicles that are used in different Use Case categories, different communication media may be required (PLC, Wireless, RFID etc)
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Field	ENUM	Description
ID	No	189.EPIC.FINSENY.Service/Function.Support of different SLAs of network infrastructure
Name	No	Support of different SLAs of network infrastructure
Goal	No	The network infrastructure should feature numerous levels of SLA's, the best being guaranteed QoS, the worst being best effort QoS.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	
Status	Yes	
MoSCoW priority	Yes	SHOULD
Relative priority	No	SHOULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The network infrastructure should feature numerous levels of SLA's, the best being guaranteed QoS, the worst being best effort QoS.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	27/07/2011
Last modified	No	27/07/2011

Field	ENUM	Description
ID	No	195.EPIC.FINSENY.Service/Function.Billing and Payment Mechanism
Name	No	Billing and Payment Mechanism
Goal	No	The Billing and Payment Systems allows manage the information required by the user to make a transaction.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	The EVSE access device (card/key fob or mobile) holds details on credit amount available to the EV User. The EVSE should have a way for completing a mobile, m-payment through a CSP The EVSE has a pay as you go system, where the EV User can top their credit on a EVSE Access card. The charge point provides multiple payment options - cash, card, deferred payment (credited to an account). converged energy and communications billing systems should support micro transactional services
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The Billing and Payment Systems allows manage the information required by the user to make a transaction.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Field	ENUM	Description
ID	No	204.EPIC.FINSENY.Service/Function.Performance Management
Name	No	Performance Management
Goal	No	Performance management ensures that SLA are being met in an effective and efficient manner. Performance management can focus on the performance of any ICT component of the Grid..
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	A real time application (like Telecontrol Function) is featured because a delay in the communications has similar effects than a lost. The use of a cloud computing is mandatory to satisfy the high performance needed in this scenario. Using a cloud of HW/SW resources the requested information are so quickly provided to computers and other devices over Internet. Grid users, Service providers and customers would have to connect via web based interfaces to the eMarket4E services.
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Performance management ensures that SLA are being met in an effective and efficient manner. Performance management can focus on the performance of any ICT component of the Grid..
Rationale	No	One of the typical operations of MV-DAC from the utility control centre use case is to switch off and switch of an electrical line that feed an area. It is very important that all ICT elements that provide the Telecontrol Function have batteries with a suitable autonomy in order to not be affected by these typical operations. As an example, the Telecontrol Function is implemented by means of a periodical polling, each 2 seconds. This period is related mainly by the latency of the physical medium. When using specific physical mediums for example geostationary satellite mediums, these periodical polling should be longer (each 3 seconds for example). The effect of this is that when a grid operator sends an order, receives the updated information in the grid control application in less than this configured period. Jitter must be controlled in any case. When an answer arrives after the periodical polling period, a communication error arises. It has the same effect than a communication lost. Any failure, even that it is solved in a short period, spent a lot of resources in both the client and the provider.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	27/07/2011
Last modified	No	27/07/2011

Field	ENUM	Description
ID	No	203.EPIC.FINSENY.Service/Function.Simple Communication EV User - Charge Station
Name	No	Simple Communication EV User - Charge Station
Goal	No	Electric Vehicle Users (EV Users) need to specify preferences such as the Charge Time Frame and the Minimum Battery State Of Charge (BSOC). This can be done in the simplest case by means of a touch screen at the charge station.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Usability
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Electric Vehicle Users (EV Users) need to specify preferences such as the Charge Time Frame and the Minimum Battery State Of Charge (BSOC). This can be done in the simplest case by means of a touch screen at the charge station.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Field	ENUM	Description
ID	No	221.EPIC.FINSENY.Service/Function.Varying Energy suppliers at one Public Charge Point
Name	No	Varying Energy suppliers at one Public Charge Point
Goal	No	Different energy suppliers use the same charging point to deliver their services.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Interoperability
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Different energy suppliers use the same charging point to deliver their services.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	09/06/2011
Last modified	No	09/06/2011

Field	ENUM	Description
ID	No	222.EPIC.FINSENY.Service/Function.Derivation of energy prices
Name	No	Derivation of energy prices
Goal	No	Energy providers need to be able to dynamically derive energy prices for the next hours. This requires precise forecasts of the availability of energy, as well as of the expected demand. Dynamic prices are then a means to balance the energy need and to avoid potentially expensive peaks of the demand.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Energy providers need to be able to dynamically derive energy prices for the next hours. This requires precise forecasts of the availability of energy, as well as of the expected demand. Dynamic prices are then a means to balance the energy need and to avoid potentially expensive peaks of the demand.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Field	ENUM	Description
ID	No	230.EPIC.FINSENY.Service/Function.Interfaces
Name	No	Interfaces
Goal	No	The interfaces for all users should be easy-understandable and user-friendly.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Diverse preferences and abilities of the customers should be taken into account when designing the service interaction of eMarket4E services. The interfaces for all users should be easy-understandable and user-friendly. If not, users would not use the advanced systems. The display (HMI) of the grid control application to the grid operator has to be clear and intuitive, providing maximum usability, as it may be used in stressing situations. In case of Demand Side Management, the tariff/price information received from the network has to be understandable both by the automatic home/building energy management system and by the customer (person) .
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The interfaces for all users should be easy-understandable and user-friendly.
Rationale	No	Understandable user interfaces may affect customers' involvement. Final customer's acceptance is key and thus flexibility in the user access interfaces should be provided.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/08/2011
Last modified	No	22/08/2011

Field	ENUM	Description
ID	No	238.EPIC.FINSENY.Service/Function.Transactional mechanisms
Name	No	Transactional mechanisms
Goal	No	The actions of "offering Energy " and "buying Energy " are meant as ICT transactions between the prosumer and Green Market Operator.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	The action of "trading energy" have to be meant as ICT transactions. Closing contracts should be done giving transactional guarantees.
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The actions of “offering Energy " and "buying Energy " are meant as ICT transactions between the prosumer and Green Market Operator.
Rationale	No	As the most part of eMarketplace in other domains, also the exchange of energy should be performed in a transactional way.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/08/2011
Last modified	No	22/08/2011

Field	ENUM	Description
ID	No	257.EPIC.FINSENY.Service/Function.eMarket4E services
Name	No	eMarket4E services
Goal	No	The services that will be provided at the eMarket4E will have to comply with: Ease of learning, memorable, maintenance, natural interaction and user satisfaction. This refers to the service interaction design in one side (service provider) and on the other by the artefacts provided at the platform side to mash up and produce services.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	An electronic marketplace needs to be available that facilitates management, collection and selection of grid issues and issue solution (offers) as well as the management, recommendation, negotiation and closing of energy (shifting) contracts and notification services and reporting. The service also will hold user energy information in detail. And it has to feature the capability of personalizing the interface depending on the context and preferences of the users. A WEB based information service dedicated to the very small energy retailers providing them the pricing Information, the present local demand and the available energy to bid. Moreover it performs forecasts for the future energy demand coming from the Facility Manager or the Final Customer. A WEB portal that allows to the final user, through a smart phone or a PC, to choose between different energy retailer in order to get at best, technically and economically, its energetic needs. The contract negotiation, act of offering energy surplus and act of buying energy surplus should be designed following web-service API, so that different application (including web-based ones) can be developed for different devices. The Service at the marketplace will have to implement complex operations between the data that will be collected from the Grid users and operators. These services that may lie on the Grid User side or in the cloud needs to know the user contract and the installed capabilities. According to the latter processing capabilities are key to decide how to signal the shape demand commends. Additional services like Weather Forecast can be provided to the Operations Manager or to the Energy Information Provider: this can be very useful for to make forecasts about the energy sources depending from wind, sun etc.
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The services that will be provided at the eMarket4E will have to comply with: Ease of learning, memorable, maintainable, natural interaction and user satisfaction. This refers to the service interaction design in one side (service provider) and on the other by the artefacts provided at the platform side to mash up and produce services.
Rationale	No	An electronic marketplace needs to be available that facilitates management, collection and selection of grid issues and issue solution (offers) as well as the management, recommendation, negotiation and closing of energy (shifting) contracts and notification services and reporting. The service also will hold user energy information in detail. And it has to feature the capability of personalizing the interface depending on the context and preferences of the users.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	24/08/2011
Last modified	No	24/08/2011

Field	ENUM	Description
ID	No	290.EPIC.FINSENY.Service/Function.High portability applications for fixed and mobile services targeted to the final customer
Name	No	High portability applications for fixed and mobile services targeted to the final customer
Goal	No	The applications for the services about the eMarket4E have to function properly on the widest possible range of devices, whether they are fixed or mobile, with different operating systems.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	This requirement is mandatory because the type of devices used by end users is quite varied: it's the service that must adapt to the customer and not vice versa
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The applications for the services about the eMarket4E have to function properly on the widest possible range of devices, whether they are fixed or mobile, with different operating systems.
Rationale	No	This requirement is mandatory because it's the service that must adapt to the customer devices and not vice versa
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	20/09/2011
Last modified	No	20/09/2011

Field	ENUM	Description
ID	No	291.EPIC.FINSENY.Service/Function.Real time system to monitor the available kind of energy for the energy retailers
Name	No	Real time system to monitor the available kind of energy for the energy retailers
Goal	No	A SW WEB-based system that allow to the energy retailers to give the kind of requested energy together at all the necessary market information
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	The knowledge of the kind of energy should be also available in mobility through the use of Smartphone, laptop, PC etc. connected to the Internet
Status	Yes	
MoSCoW priority	Yes	SHOULD
Relative priority	No	SHOULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	A SW WEB-based system that allow to the energy retailers to give the kind of requested energy together at all the necessary market information
Rationale	No	This requirement is mandatory to monitor in the real time the available kind of energy for the energy retailers
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	26/08/2011
Last modified	No	26/08/2011

Field	ENUM	Description
ID	No	292.EPIC.FINSENY.Service/Function.Grid/Network Management
Name	No	Grid/Network Management
Goal	No	The companies responsible for the management of the network must have tools that allow them to handle the available information and predict contingences.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	The networking of different kinds of energy requires reliable apparatus that are able to synchronize phases and frequencies to the values provided by the regulations. NMS protocols (e.g. SNMP, at least SNMP v1, SNMP v2 could be supported, SNMP v3 support is desirable.) Visualization tool. Each smart meter has to be connected with a radio device (e.g. ZigBee node) in order to send the collected data in wireless mode. Since almost real-time dynamic tariff schemes should be targeted, data volume will be high, and the management of the related contracts would be demanding because of the potential high amount of users.
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The companies responsible for the management of the network must have tools that allow them to handle the available information and predict contingences.
Rationale	No	This requirement is mandatory to have different sources of energy for an ethical choice by the end user
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	26/08/2011
Last modified	No	26/08/2011

Field	ENUM	Description
ID	No	298.EPIC.FINSENY.Service/Function.Scalability
Name	No	Scalability
Goal	No	Scalability is the guarantee that a system can grow without compromising its operations.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Scalability of the IT (central and mobile) systems to allow for system application and I/F-type expansion between Central Dispatch System (CSD) and Field Mobile Devices (FMD) needs: Scalability of the IT systems in terms of - Processing and data base handling capacity and to allow for system expansion incl. - Adaptation to new physical I/Fs: - LTE/4G and UMTS/3G (e.g. for regular operation), - 2G/GPRS – low speed, - WiFi Internet access via Hotspots, - Satellite Links via public or privately operated networks - Direct Ethernet to connect into public networks - Direct Ethernet to connect into substation networks - DSL (ADSL) modem connection to public operators via twisted pairs (assuming no local power, but central office DSLAM power back-up) - Powerline communications (PLC/BPL to Low Voltage data networks, i.e. into Smart Meter Field Area Communication networks - FAN) - Local Mesh Radio communications (ZigBee, Z-Wave, i.e. into Smart Meter Field Area Communication networks - FAN) - New applications, tailored to the above communication capabilities
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Scalability is the guarantee that a system can grow without compromising its operations.
Rationale	No	The Requirement is mandatory to be able to provide the service. High processing demand is needed to fine-grained forecasting at e-Island level. More, the volume of instant data is very high, due the amount of distributed sources. A marketplace makes only sense when it can handle the transactions of all (potential) market participants.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	09/09/2011
Last modified	No	09/09/2011

Field	ENUM	Description
ID	No	312.EPIC.FINSENY.Service/Function.Monitoring and control user interfaces for building end-users
Name	No	Monitoring and control user interfaces for building end-users
Goal	No	User Interfaces for building end-users have to be proposed in at least two different ways : as fixed interfaces inside the building, possibly using a dedicated interface devices (like a home/building control panel), and as either mobile or generic remote interfaces. This duality makes it almost mandatory that the support of these interfaces be available outside of the home network, which will also make it easier for third parties to have access to their own user interfaces
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Usability
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	User Interfaces for building end-users have to be proposed in at least two different ways : as fixed interfaces inside the building, possibly using a dedicated interface devices (like a home/building control panel), and as either mobile or generic remote interfaces. This duality makes it almost mandatory that the support of these interfaces be available outside of the home network, which will also make it easier for third parties to have access to their own user interfaces
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Field	ENUM	Description
ID	No	313.EPIC.FINSENY.Service/Function.Monitoring, control and management user interfaces for technical staff, facilities managers, etc
Name	No	Monitoring, control and management user interfaces for technical staff, facilities managers, etc
Goal	No	Similar to interfaces for building inhabitants, and excluding the case of homes, these do generally have to be available through fixed or dedicated devices inside the building, and, possibly with reduced functionality, as interfaces outside the building. Similar arguments apply to the support of these interfaces outside the building network.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Usability
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Similar to interfaces for building inhabitants, and excluding the case of homes, these do generally have to be available through fixed or dedicated devices inside the building, and, possibly with reduced functionality, as interfaces outside the building. Similar arguments apply to the support of these interfaces outside the building network.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	21/09/2011
Last modified	No	21/09/2011

10.2 Information Layer

Field	ENUM	Description
ID	No	23.EPIC.FINSENY.Information.Persistent data storage
Name	No	Persistent data storage
Goal	No	SG devices must contain enough non-volatile memory (e.g. flash memory) for storing measurements, internal data, and enable future firmware and software updates.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	

Scope	Yes	Robustness
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	SG devices must contain enough non-volatile memory (e.g. flash memory) for storing measurements, internal data, and enable future firmware and software updates.
Rationale	No	This requirement relates to most of the embedded devices of SG system.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	08/06/2011
Last modified	No	08/06/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	41.EPIC.FINSENY.Information.Data management
Name	No	Data management
Goal	No	The use case involves handling (processing, analyzing, semantically classifying and accessing) large volumes of data that partially have to be stored for later use (e.g. billing, planning, historical analysis, regulation). The data must be kept consistent and synchronized with other systems within seconds. Data consistency has to be executed by DMS/SCADA system
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Visualization tool
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The use case involves handling (processing, analyzing, semantically classifying and accessing) large volumes of data that partially have to be stored for later use (e.g. billing, planning, historical analysis, regulation). The data must be kept consistent and synchronized with other systems within seconds. Data consistency has to be executed by DMS/SCADA system
Rationale	No	Data management is required in order to maintain operational consistency
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	24/06/2011
Last modified	No	24/06/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	42.EPIC.FINSENY.Information.Data values checking
Name	No	Data values checking
Goal	No	The use cases involve monitoring and otherwise retrieving large amounts of data from different parts of the distribution network. The data integrity ensures that there is no tampering with the data but still there could be problems e.g. with sensors. Malfunctioning devices of the SG could produce data that should not be accepted by the receiving entity. This can be considered as a certain kind of sanity check, but it can also be utilized with fault detection procedures. This is a requirement for the application level of the SG system software.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Is always application dependent.
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The use cases involve monitoring and otherwise retrieving large amounts of data from different parts of the distribution network. The data integrity ensures that there is no tampering with the data but still there could be problems e.g. with sensors. Malfunctioning devices of the SG could produce data that should not be accepted by the receiving entity. This can be considered as a certain kind of sanity check, but it can also be utilized with fault detection procedures. This is a requirement for the application level of the SG system software.
Rationale	No	Unacceptable data values must be detected in order to prevent undesirable application behavior and to notify the system of possible malfunctioned equipment.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	08/08/2011
Last modified	No	08/08/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	58.EPIC.FINSENY.Information.Data bus
Name	No	Data bus
Goal	No	The data bus should provide different communication services (e.g. request/response, publish/subscribe, transactions). Furthermore, it should support different levels of Quality of Service because different applications have different demands, e.g. w.r.t. latency, frequency of data exchange, quality or time synchronization.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Robustness
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The data bus should provide different communication services (e.g. request/response, publish/subscribe, transactions). Furthermore, it should support different levels of Quality of Service because different applications have different demands, e.g. w.r.t. latency, frequency of data exchange, quality or time synchronization.
Rationale	No	The Microgrid's Data Management System classifies, processes, correlates and filters the monitored data, and provides meaningful state information of the Microgrid which in turn can be used by all control and management applications.Transforming and analyzing this data into useful business and operational intelligence is one of the biggest challenges for the Microgrid. For this purpose a flexible service bus supporting Quality of Service is crucial.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	02/09/2011
Last modified	No	02/09/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	59.EPIC.FINSENY.Information.Database system
Name	No	Database system
Goal	No	A central or local (distributed) database system is required to provide storage system(s) for context information (EV users, EVSE, environmental 3rd party). In an EVSE, also a local database may be used for charge detailled record.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Data has to be stored persistently in a database (e.g. for archiving and post-mortem analysis). The database system has to show high-performance because of the high volume of data and multiple access. Furthermore, the database should support structured and unstructured data and should provide flexible query functionalities. Examples for data storage in the electromobility environment are: tariffs, battery and auxillary data, geo-location information. user profiles, weather and topology information etc.
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	A central or local (distributed) database system is required to provide storage system(s) for context information (EV users, EVSE, environmental 3rd party). In an EVSE, also a local database may be used for charge detailled record.
Rationale	No	E.g., switching network configuration to and from Islanding Mode needs for Optimal Power Flow, to initiate and configure the new context.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	02/09/2011
Last modified	No	02/09/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	62.EPIC.FINSENY.Information.Distributed Processing
Name	No	Distributed Processing
Goal	No	For balancing supply and demand the Microgrid Control Center has to run the state analysis and define the sub-sequent actions. These tasks include power flow calculations and forecasting models. To minimize processing latency the jobs could be processed in parallel and distributed across different machines.Also for forecasting, planning and revenue in the revenue distributed processing capabilities are crucial.

Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Robustness
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	For balancing supply and demand the Microgrid Control Center has to run the state analysis and define the sub-sequent actions. These tasks include power flow calculations and forecasting models. To minimize processing latency the jobs could be processed in parallel and distributed across different machines.Also for forecasting, planning and revenue in the revenue distributed processing capabilities are crucial.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	63.EPIC.FINSENY.Information.High Demand for Computing Resources / Processing
Name	No	High Demand for Computing Resources / Processing
Goal	No	For some use cases, it is necessary to provide high performance computing resources for calculation and simulation models in the Microgrid Control Centre including real-time processing.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Robustness
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	

Category	Yes	
Description	No	For some use cases, it is necessary to provide high performance computing resources for calculation and simulation models in the Microgrid Control Centre including real-time processing.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	64.EPIC.FINSENY.Information.Demand management based on criticality of loads
Name	No	Demand management based on criticality of loads
Goal	No	MG management and control system shall control loads and enable smart load controlling (cancellation of loads, shifting if loads etc.).
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Robustness
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	MG management and control system shall control loads and enable smart load controlling (cancellation of loads, shifting if loads etc.).
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	95.EPIC.FINSENY.Information.Common data models (CDM)
Name	No	Common data models (CDM)
Goal	No	Definition of common data models (CDM) per type of sensor/appliance. In order to perform energy optimization on behalf of the consumer, home appliances must be modelled in a common way so that the intelligence in the system is able to monitor them, know control capabilities, programming capabilities and have at any moment information on the reachability of the device.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Robustness
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Definition of common data models (CDM) per type of sensor/appliance. In order to perform energy optimization on behalf of the consumer, home appliances must be modelled in a common way so that the intelligence in the system is able to monitor them, know control capabilities, programming capabilities and have at any moment information on the reachability of the device.
Rationale	No	Energy Efficiency Service try to optimize energy use so that only the minimum energy required is spent to have the desired service.Common Data Models are necessary to offer appliance/sensor manufacturers the minimum set of functionalities that the devices should implement to be used by efficiency services.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	21/09/2011
Last modified	No	21/09/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	109.EPIC.FINSENY.Information.Check Energy Use
Name	No	Check Energy Use
Goal	No	Availability of access to data of current status of the building shall be guaranteed both locally and remotely from Internet connected devices 95% of time
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Robustness
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Availability of access to data of current status of the building shall be guaranteed both locally and remotely from Internet connected devices 95% of time
Rationale	No	In order to ensure the most critical functionalities derived from other requirements, such as the remote alert management, a very high availability rate of the system must be guaranteed
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	21/09/2011
Last modified	No	21/09/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	151.EPIC.FINSENY.Information.Reliability
Name	No	Reliability
Goal	No	Data transmission has to be reliable
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Robustness
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Data transmission has to be reliable
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	152.EPIC.FINSENY.Information.Reliable data transport over heterogeneous networks
Name	No	Reliable data transport over heterogeneous networks
Goal	No	Different Communication Service Providers (CSP) are maybe involved in a single data transaction. End-2-End QoS has to be assured over CSP boundaries including identification of Location of Failure.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Robustness
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Different Communication Service Providers (CSP) are maybe involved in a single data transaction. End-2-End QoS has to be assured over CSP boundaries including identification of Location of Failure.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	159.EPIC.FINSENY.Information.Data integrity
Name	No	Data integrity
Goal	No	In particular for all payment scenarios, data integrity has to be ensured.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Robustness
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	In particular for all payment scenarios, data integrity has to be ensured.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	161.EPIC.FINSENY.Information.Low latency of data transmissions for V2G / G2V
Name	No	Low latency of data transmissions for V2G / G2V
Goal	No	The information exchange for grid stabilizing purpose has to be quasi real-time
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Robustness
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The information exchange for grid stabilizing purpose has to be quasi real-time
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	162.EPIC.FINSENY.Information.Low latency of data transmissions for Stored Energy Services
Name	No	Low latency of data transmissions for Stored Energy Services
Goal	No	The information exchange for grid stabilizing purpose has to be quasi real-time
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	The use of a cloud computing is mandatory to satisfy the high performance needed in this scenario. Using a cloud of HW/SW resources the requested information are so quickly provided to computers and other devices over Internet.
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The information exchange for grid stabilizing purpose has to be quasi real-time
Rationale	No	This is an essential requirement and the system will not work properly without it.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	165.EPIC.FINSENY.Information.Data management for VAS
Name	No	Data management for VAS
Goal	No	High amounts of data have to be stored and evaluated
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Robustness.
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	High amounts of data have to be stored and evaluated
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	166.EPIC.FINSENY.Information.Data management for V2G / G2V
Name	No	Data management for V2G / G2V
Goal	No	High amounts of data have to be stored and evaluated in order to allow for grid integration services
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Robustness
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	High amounts of data have to be stored and evaluated in order to allow for grid integration services
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	168.EPIC.FINSENY.Information.Data throughput for ES
Name	No	Data throughput for ES
Goal	No	High data throughput has to be ensured for all kinds of enhanced Services when high numbers of EV are used
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Robustness
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	High data throughput has to be ensured for all kinds of enhanced Services when high numbers of EV are used
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	236.EPIC.FINSENY.Information.Data integrity
Name	No	Data integrity
Goal	No	The data to be trasmissed and received have to be reliable in term of truthfulness and timing. The transmitted and received data has to be reliable.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Security, Robustness, Performance
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The data to be trasmissed and received have to be reliable in term of truthfulness and timing. The transmitted and received data has to be reliable.
Rationale	No	This is an essential requirement and the system will not work properly without it.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/08/2011
Last modified	No	22/08/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	253.EPIC.FINSENY.Information.Data management and storage
Name	No	Data management and storage
Goal	No	Large amounts of data need to be collected, stored and made available.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Security, Robustness, Performance
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Large amounts of data need to be collected, stored and made available.
Rationale	No	This is an essential requirement and the system will not work properly without it.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	29/08/2011
Last modified	No	29/08/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	288.EPIC.FINSENY.Information.Cloud computing for high speed data processing
Name	No	Cloud computing for high speed data processing
Goal	No	To exchange in real time: pricing Information, present demand, available energy to bid and forecast for the future energy demand, a large amounts of data need to be collected and processed in high speed mode through cloud computing.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	The use of a cloud computing is mandatory to satisfy the high performance needed in this scenario. Using a cloud of HW/SW resources the requested information are so quickly provided to computers and other devices over Internet.
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	To exchange in real time: pricing Information, present demand, available energy to bid and forecast for the future energy demand, a large amounts of data need to be collected and processed in high speed mode through cloud computing.
Rationale	No	This is an essential requirement and the system will not work properly without it.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	20/09/2011
Last modified	No	20/09/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	296.EPIC.FINSENY.Information.Building data transmission availability
Name	No	Building data transmission availability
Goal	No	The BEMS installed at the user premises will have to transmit data over the Internet. Always on connectivity and ADSL speeds are required and on the provider side (Marketplace) Data Mining will thus apply.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	This scenario will require real -time communication. Reliability should be high although high bandwidth is not needed. The data distribution will be regular over a 24h period.
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The BEMS installed at the user premises will have to transmit data over the Internet. Always on connectivity and ADSL speeds are required and on the provider side (Marketplace) Data Mining will thus apply.
Rationale	No	The Requirement is mandatory to be able to provide the service.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	09/09/2011
Last modified	No	09/09/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	298.EPIC.FINSENY.Information.Data Integrity at the MarketPlace
Name	No	Data Integrity at the MarketPlace
Goal	No	The Information that is to be collected by the Marketplace has to be handled taking care of personalizationn and context based information.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	The volume of instant data is not high. But large amounts of data are to be saved on a server. Context management is key to determine information of various devices well identified. A high number of parameters will be needed for the profile of customers and devices.
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The Information that is to be collected by the Marketplace has to be handled taking care of personalizationn and context based information.
Rationale	No	The Requirement is mandatory to be able to provide the service.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	09/09/2011
Last modified	No	09/09/2011

10.3 Communication Layer

Field	ENUM	Description
ID	No	10.EPIC.FINSENY.Communication.Reliability and availability on Communications Technology (CT) layer
Name	No	Reliability and availability on Communications Technology (CT) layer
Goal	No	Reliability of CT layer I/Fs towards Aggregator, VPP or DSO and SG-devices.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Insuring reliability and defining a suitable availability of CT operations towards Aggregator, VPP or DSO processes, applications, databases and the SG-devices.
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Reliability of CT layer I/Fs towards Aggregator, VPP or DSO and SG-devices.
Rationale	No	Defining availability figures on CT layer is relevant for ongoing operation and also related to safe grid operation
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	04/07/2011
Last modified	No	04/07/2011

Field	ENUM	Description
ID	No	11.EPIC.FINSENY.Communication.Handover Management
Name	No	Handover Management
Goal	No	The communication handset device used by field worker to synchronize work orders should have the availability to manage the handover between several commutations media in a transparent way. The best media should be selected regarding the QoS needed in term of latency, jitter and bandwidth. In case of a crisis situation (a tempest for example), a crisis media (such as Private Mobile Radio) should be available for data communication with the same handset device used by workers during “normal” situation.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Performance, Robustness
Status	Yes	
MoSCoW priority	Yes	SHOULD
Relative priority	No	SHOULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The communication handset device used by field worker to synchronize work orders should have the availability to manage the handover between several commutations media in a transparent way. The best media should be selected regarding the QoS needed in term of latency, jitter and bandwidth. In case of a crisis situation (a tempest for example), a crisis media (such as Private Mobile Radio) should be available for data communication with the same handset device used by workers during “normal” situation.
Rationale	No	Multihoming with automatic handover management will enhance the possibility for a worker to have access to central data, especially in a crisis situation
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	01/07/2011
Last modified	No	01/07/2011

Field	ENUM	Description
ID	No	12.EPIC.FINSENY.Communication.IP mobility
Name	No	IP mobility
Goal	No	From the Dispatch System point of view, the communication system must be able to "push" data to the worker handset whatever the telecommunication medium the worker is currently using, even if its IP address has changed.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Performance, Robustness
Status	Yes	
MoSCoW priority	Yes	SHOULD
Relative priority	No	SHOULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	From the Dispatch System point of view, the communication system must be able to "push" data to the worker handset whatever the telecommunication medium the worker is currently using, even if its IP address has changed.
Rationale	No	IP mobility is an issue that must be handled by the communication system
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	08/07/2011
Last modified	No	08/07/2011

Field	ENUM	Description
ID	No	13.EPIC.FINSENY.Communication.Adaptation of application to available bandwidth
Name	No	Adaptation of application to available bandwidth
Goal	No	If a low bandwidth media is used (for example in the case of a crisis situation after a tempest), the central IS Dispatch System must adapt its response according to the bandwidth available: only the core data of the work order are sent and not the attached files.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Performance, Robustness
Status	Yes	
MoSCoW priority	Yes	SHOULD
Relative priority	No	SHOULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	If a low bandwidth media is used (for example in the case of a crisis situation after a tempest), the central IS Dispatch System must adapt its response according to the bandwidth available: only the core data of the work order are sent and not the attached files.
Rationale	No	Application plasticity will be very helpful especially during crisis situation in order to be able to send data to the field workers.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	18/09/2011
Last modified	No	18/09/2011

Field	ENUM	Description
ID	No	21.EPIC.FINSENY.Communication.Request/Response
Name	No	Request/Response
Goal	No	Data will be sent on a request, when a system is asking for a certain information and the Data Provider response back to that system with requested information or at least acknowledging the request.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Performance, Robustness
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Data will be sent on a request, when a system is asking for a certain information and the Data Provider response back to that system with requested information or at least acknowledging the request.
Rationale	No	Request-response or request-reply is one of the basic methods computerized systems use to talk to each other. When using request-response, the first system requests some data and the second system responds to the request.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	05.08.2011
Last modified	No	05.08.2011

Field	ENUM	Description
ID	No	22.EPIC.FINSENY.Communication.Time synchronization
Name	No	Time synchronization
Goal	No	To achieve network wide synchronization of control tasks on different time-ranges and scalability up to hundreds of systems, while being robust to topology changes and failures, a time-based synchronization method by utilizing concepts of e.g. time-stamping and skew compensation with linear regression is needed.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Performance, Robustness
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	To achieve network wide synchronization of control tasks on different time-ranges and scalability up to hundreds of systems, while being robust to topology changes and failures, a time-based synchronization method by utilizing concepts of e.g. time-stamping and skew compensation with linear regression is needed.
Rationale	No	Certain types of control applications require synchronized action sequences, on one hand for stringent and fast aligned control tasks (no jitter) or on the other for completing control tasks under upper limits of time.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	05.08.2011
Last modified	No	05.08.2011

Field	ENUM	Description
ID	No	26.EPIC.FINSENY.Communication.Priority
Name	No	Priority
Goal	No	Priority in transmission scheduling is an easy way to prefer data of one connection compared to other connections.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Performance, Robustness
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Priority in transmission scheduling is an easy way to prefer data of one connection compared to other connections.
Rationale	No	The remote control traffic should be prioritized over any other, afterwards the monitoring and metering traffic and finally the traffic dedicated to measurements.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	05.08.2011
Last modified	No	05.08.2011

Field	ENUM	Description
ID	No	30.EPIC.FINSENY.Communication.Latency
Name	No	Latency
Goal	No	The communication infrastructure must offer a guarantee on the maximal round trip time for messages (from the application on the originator device to the destination device and back)
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Support real time requirements of DCAC, FLIR, MWFM, SGEC: latency of at most 1 sec
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The communication infrastructure must offer a guarantee on the maximal round trip time for messages (from the application on the originator device to the destination device and back)
Rationale	No	FLIR: In order to comply with standards (CEI, IEEE) FLIR is required to complete restoration within one minute. Since several messages have to be disseminated during the process, a delay of at most one second is acceptable. For teleprotection a delay of at most 50ms must be guaranteed. Since the voltages are much lower in the distribution network than in the transmission network, teleprotection is less important here than in transmission networks and we can omit the harsh requirement that only <50ms latency is acceptable (nice to have, but requires a large effort). MWFM: To react timely to new situations, field workers need to be notified of important events within seconds DCAC, SGEC: Control applications require fine-grained updates on state and fast delivery of commands, the typical latency requirement is one second. Some system critical components might require faster communication for network stability.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	27/06/2011
Last modified	No	27/06/2011

Field	ENUM	Description
ID	No	33.EPIC.FINSENY.Communication.Bandwidth allocation
Name	No	Bandwidth allocation
Goal	No	Bandwidth ~ 100 kbps
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Not applicable
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Bandwidth ~ 100 kbps
Rationale	No	The delivery of real time information for FLIR, DCAC and SGEC requires the timely exchange of several hundreds of bytes. For MWFM applications with maps require a suitable bandwidth to support the field workers.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Field	ENUM	Description
ID	No	34.EPIC.FINSENY.Communication.Packet Loss
Name	No	Packet Loss
Goal	No	Packet loss here means the maximum acceptable percentage of lost packets on a communication link. The lost packets may be retransmitted (reducing the goodput) or not. In the latter case the acceptable packet loss rate means the number of lost packets that would allow the receiving endpoint to realize the communication with a quality that may still be acceptable for the user (i.e. in video transmission: with which percentage of lost packets a video transmission may still be reasonable for the user at the receiving end?)
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Packet Lost defines the maximum level of errors that the application could manage for normal operation. This parameter affects more drastically to Telecontrol function.
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Packet loss here means the maximum acceptable percentage of lost packets on a communication link. The lost packets may be retransmitted (reducing the goodput) or not. In the latter case the acceptable packet loss rate means the number of lost packets that would allow the receiving endpoint to realize the communication with a quality that may still be acceptable for the user (i.e. in video transmission: with which percentage of lost packets a video transmission may still be reasonable for the user at the receiving end?)
Rationale	No	If packet lost is high Grid Control application becomes not so interactive as designed and safety problems could arise when switching circuit breakers
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	23/06/2011
Last modified	No	23/06/2011

Field	ENUM	Description
ID	No	38.EPIC.FINSENY.Communication.High priority asynchronous messages
Name	No	High priority asynchronous messages
Goal	No	In case of alarms, e.g. in conjunction with power inverters, the according asynchronous messages must be transported very fast to the controller, as alarms normally reflects a very soon loss of energy production. In order to further guarantee the stability of the smart grid, therefore, this information must be transported with highest priority or via reserved communication channels. Without time-synchronization just the priority of the (asynchronous) telegram can be used to reduce the latency from submitting the message until receiving it.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Establish prioritized communication channels Fast priority routing mechanisms Security Means Interoperability of the IT-System on North-bound IT I/Fs. (Wrt processes, applications and databases in the sense of CIM/IEC61968, GID/IEC61970, GIS and Interactions) founded on available standards and extensions. Interoperability on standardized South-bound IT I/Fs as IEC61850, IEC60870, DNP3 used for control and alarm purposes of SG-devices, DER, DG, Storage and SGEC devices.
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	In case of alarms, e.g. in conjunction with power inverters, the according asynchronous messages must be transported very fast to the controller, as alarms normally reflects a very soon loss of energy production. In order to further guarantee the stability of the smart grid, therefore, this information must be transported with highest priority or via reserved communication channels. Without time-synchronization just the priority of the (asynchronous) telegram can be used to reduce the latency from submitting the message until receiving it.
Rationale	No	In order to be able to stabilize the grid even in case of big energy losses as a consequence of a failure situation (e.g. within an DER) the controller must be informed immediately about the new situation. The controller then is forced to use such high priority channels in order to redirect energy to maintain stability of the grid.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	24/06/2011
Last modified	No	24/06/2011

Field	ENUM	Description
ID	No	72.EPIC.FINSENY.Communication.Latency
Name	No	Latency
Goal	No	For each Function/Service/Application, the right level of latency must be guaranteed.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Round-trip between service platform (used for remote data processing and storage) and local platform must be stricly bounded for a fewsafety critical functions
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	For each Function/Service/Application, the right level of latency must be guaranteed.
Rationale	No	The Balancing and Ancillary markets (BUC-2) would operate in minutes delay range, so in this case the latency will not be critical. The latency requirement for monitoring and remote control tasks (CUC-1) in conventional electrical networks is about tenths of a second, and so should be for Microgrids. If in the future Microgrids plan to carry out security duties, the maximum tolerated latency would be about a few milliseconds. Consumers must be aware that the control commands they have demanded over the appliances have get the corresponding answer over the appliances. For that reason a maximum time of response is needed. Otherwise the user would think that the command has not been sent and probably will send it again.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	05/08/2011
Last modified	No	05/08/2011

Field	ENUM	Description
ID	No	73.EPIC.FINSENY.Communication.Bandwidth, Throughput, Goodput
Name	No	Bandwidth, Throughput, Goodput
Goal	No	For each Function/Service/Application, the right level of bandwith, troughput and goodput must be guaranteed.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Performance, Robustness
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	For each Function/Service/Application, the right level of bandwith, troughput and goodput must be guaranteed.
Rationale	No	Conventional Monitoring, Metering and Remote control task in electrical are not High Bandwidth demanding, 128 Kbits are more than enough in most cases. Only the main points of the networks, as the control centers demand more bandwidth, but even in this case 2 or 4 Mbits are enough. New standards like IEC 61850 are more bandwidth requesting, but even in this case, the nowadays communications networks are ready to satisfy those requirements. There are different requirements for the different use cases, almost all required medium or low bandwidth. The exact values (i.e. what does low / medium / high bandwidth really mean?) will be defined later. The biggest amount of data exchanged between the gateway and the service platform will happen when the customer connects remotely to real time energy monitoring applications.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	05/08/2011
Last modified	No	05/08/2011

Field	ENUM	Description
ID	No	74.EPIC.FINSENY.Communication.Publish / Subscribe
Name	No	Publish / Subscribe
Goal	No	In asynchronous messaging a system places a message in a message queue based on internal logic or event and does not need to wait for a reply to continue processing. Subscribers express interest in one or more message classes, and only receive messages that are of interest for them.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Performance, Robustness
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	In asynchronous messaging a system places a message in a message queue based on internal logic or event and does not need to wait for a reply to continue processing. Subscribers express interest in one or more message classes, and only receive messages that are of interest for them.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	05/08/2011
Last modified	No	05/08/2011

Field	ENUM	Description
ID	No	82.EPIC.FINSENY.Communication.Error detection, error correction
Name	No	Error detection, error correction
Goal	No	The data link layer must provide sufficient error detection and/or error correction.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	ARQ, FEC scheme
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The data link layer must provide sufficient error detection and/or error correction.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	18/09/2011
Last modified	No	18/09/2011

Field	ENUM	Description
ID	No	84.EPIC.FINSENY.Communication.Always on
Name	No	Always on
Goal	No	There must be an always on connectivity of selected elements.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Performance, Robustness
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	There must be an always on connectivity of selected elements.
Rationale	No	Energy efficiency services should run in a local equipment in the building to ensure quality and guaranteeing that the service will be provided even in case of network failure.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	21/09/2011
Last modified	No	21/09/2011

Field	ENUM	Description
ID	No	85.EPIC.FINSENY.Communication.Connectivity
Name	No	Connectivity
Goal	No	Defines the need to “connect” in all relevant senses devices, appliances, and any physical entities that need to have a network presence inside the extended perimeter of the building management system.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Common Information Model (possibly extending the present IEC CIM) that makes it possible to assign a semantic-level identity to all relevant entities that need to be identified by the building energy management system
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Defines the need to “connect” in all relevant senses devices, appliances, and any physical entities that need to have a network presence inside the extended perimeter of the building management system.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Field	ENUM	Description
ID	No	87.EPIC.FINSENY.Communication.Coexistance of communication standards
Name	No	Coexistence of communication standards
Goal	No	Several communication standards must be able to coexist on different communication layers.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Performance, Robustness
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Several communication standards must be able to coexist on different communication layers.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	18/09/2011
Last modified	No	18/09/2011

Field	ENUM	Description
ID	No	89.EPIC.FINSENY.Communication.Loose coupling
Name	No	Loose coupling
Goal	No	The communication protocols used must be as independent as possible from particular energy functions/services/applications.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Performance, Robustness
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The communication protocols used must be as independent as possible from particular energy functions/services/applications.
Rationale	No	The home environment is heterogeneous with regards to the technologies used by the different home appliances to communicate with the 'central unit' (gateway, energy box). Cabled Ethernet, WiFi, ZigBee, Zwave, PLC based, etc, all of them are competing for the market and up to now and interoperability between technologies at application level is still missing. That is the reasoning while home energy efficiency services logic must be decoupled from the technology used by the appliances to communicate (for monitoring and control).
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	21/09/2011
Last modified	No	21/09/2011

Field	ENUM	Description
ID	No	99.EPIC.FINSENY.Communication.Join networks
Name	No	Join networks
Goal	No	The network layer must allow for the combination of two or more seperate physical networks into one logical network
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	logical combination of separate physical networks
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The network layer must allow for the combination of two or more separate physical networks into one logical network
Rationale	No	This allows managing different site as one network
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	18/09/2011
Last modified	No	18/09/2011

Field	ENUM	Description
ID	No	152.EPIC.FINSENY.Communication.Reliable data transport over heterogeneous networks
Name	No	Reliable data transport over heterogeneous networks
Goal	No	Different Communication Service Providers (CSP) are maybe involved in a single data transaction. End-2-End QoS has to be assured over CSP boundaries including identification of Location of Failure.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Performance, Robustness
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Different Communication Service Providers (CSP) are maybe involved in a single data transaction. End-2-End QoS has to be assured over CSP boundaries including identification of Location of Failure.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Field	ENUM	Description
ID	No	163.EPIC.FINSENY.Communication.Remote Upgrades
Name	No	Remote Upgrades
Goal	No	Required software upgrades of the charging station shall be possible remotely.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Performance, Robustness
Status	Yes	
MoSCoW priority	Yes	SHOULD
Relative priority	No	SHOULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Required software upgrades of the charging station shall be possible remotely.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Field	ENUM	Description
ID	No	169.EPIC.FINSENY.Communication.Multi-Communication Media
Name	No	Multi-Communication Media
Goal	No	For vehicles that are used in different Use Case categories, different communication media may be required (PLC, Wireless, RFID etc)
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Performance, Robustness
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	For vehicles that are used in different Use Case categories, different communication media may be required (PLC, Wireless, RFID etc)
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Field	ENUM	Description
ID	No	170.EPIC.FINSENY.Communication.Abstraction from Media
Name	No	Abstraction from Media
Goal	No	Despite many different access communication protocols and lots of different hardware solutions, communication must be possible
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Performance, Robustness
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Despite many different access communication protocols and lots of different hardware solutions, communication must be possible
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Field	ENUM	Description
ID	No	191.EPIC.FINSENY.Communication.Network aggregation nodes
Name	No	Network aggregation nodes
Goal	No	Aggregation nodes could be used in order to deploy present transport protocols in an efficient way.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Performance, Robustness
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Aggregation nodes could be used in order to deploy present transport protocols in an efficient way.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Field	ENUM	Description
ID	No	192.EPIC.FINSENY.Communication.Provision of Ethernet / IP bandwidth on demand services
Name	No	Provision of Ethernet / IP bandwidth on demand services
Goal	No	Aggregation nodes could be used in order to deploy present transport protocols in an efficient way.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	The network infrastructure should support the dynamic and random provision of Ethernet / IP bandwidth on demand services so that high definition uni-cast electro-mobility video services can be enabled on demand
Status	Yes	
MoSCoW priority	Yes	SHOULD
Relative priority	No	SHOULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Aggregation nodes could be used in order to deploy present transport protocols in an efficient way.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	27/07/2011
Last modified	No	27/07/2011

Field	ENUM	Description
ID	No	201.EPIC.FINSENY.Communication.Wireless coverage
Name	No	Wireless coverage
Goal	No	The level of wireless coverage should be enhanced.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Performance, Robustness
Status	Yes	
MoSCoW priority	Yes	SHOULD
Relative priority	No	SHOULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The level of wireless coverage should be enhanced.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Field	ENUM	Description
ID	No	204.EPIC.FINSENY.Communication.Advanced Communication EV User - Charge Station via Virtualization
Name	No	Advanced Communication EV User - Charge Station via Virtualization
Goal	No	The network infrastructure should feature non-blocking advanced virtualization technologies so that many virtual electro-mobility network operators can co-exist on the same physical telecoms network and dynamically scale bandwidth and network services with respect to real-time customer requirements
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Performance, Robustness
Status	Yes	
MoSCoW priority	Yes	SHOULD
Relative priority	No	SHOULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The network infrastructure should feature non-blocking advanced virtualization technologies so that many virtual electro-mobility network operators can co-exist on the same physical telecoms network and dynamically scale bandwidth and network services with respect to real-time customer requirements
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	27/07/2011
Last modified	No	27/07/2011

10.4 Component Layer

Field	ENUM	Description
ID	No	18.EPIC.FINSENY.Component.Dedicated or Shared Transport Infrastructure
Name	No	Dedicated or Shared Transport Infrastructure
Goal	No	Control from an Aggregator, VPP or DSO needs appropriate transport network capacity, which may be supplied by a dedicated operator on an exclusive or shared basis
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	South-bound IT (Server) I/Fs need to connect via suitable transport links towards the SG-device locations (e.g. Sub-Stations) Transport links may be realized via: - Optical Fibers, operating WDM, SDH/PDH, Ethernet/LAN, - 3GPP-defined cellular wireless (2G/GPRS 3G/UMTS 4G/LTE) - WIMAX or Microwave private radio network - Powerline based PLC/BPL (Powerline/Broadband Powerline Communication) - Commercial DSL-lines based on ADSL, VDSL or SHDSL
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Control from an Aggregator, VPP or DSO needs appropriate transport network capacity, which may be supplied by a dedicated operator on an exclusive or shared basis
Rationale	No	Transport infrastructure is relevant for ongoing SG operation, private or dedicated networks may be purpose designed (for reliability, security)
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	04/07/2011
Last modified	No	04/07/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	19.EPIC.FINSENY.Component.Dedicated or Shared Transport Infrastructure 2
Name	No	Dedicated or Shared Transport Infrastructure 2

Goal	No	The Communication Technology (CT) layer requires utilization of any useful link available under disturbed operating conditions. This may be supplied by a dedicated operator on an exclusive or shared basis
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	These communication technologies may be utilized: - LTE/4G / WiMAX - Satellite Links - Direct Ethernet to connect into substation networks - Powerline communications (PLC/BPL to Low Voltage data networks, i.e. into Smart Meter Field Area Communication networks - FAN) - Local Mesh Radio communications (ZigBee, Z-Wave, i.e. into Smart Meter Field Area Communication networks - FAN)
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The Communication Technology (CT) layer requires utilization of any useful link available under disturbed operating conditions. This may be supplied by a dedicated operator on an exclusive or shared basis
Rationale	No	Transport infrastructure is relevant for ongoing SG operation, private or dedicated networks may be purpose designed (for reliability, security)
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	11/07/2011
Last modified	No	11/07/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	20.EPIC.FINSENY.Component.Telco Infrastructure
Name	No	Telco Infrastructure
Goal	No	Control from an Aggregator, VPP or DSO needs appropriate transport network capacity, which may be supplied by a Telco operator
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	South-bound IT (Server) I/Fs need to connect via suitable transport links towards the SG-device locations (e.g. Sub-Stations) Transport links may be realized via: - 3GPP-defined cellular wireless (2G/GPRS 3G/UMTS 4G/LTE) - WIMAX public radio network - Public DSL-lines based on ADSL, VDSL or SHDSL
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Control from an Aggregator, VPP or DSO needs appropriate transport network capacity, which may be supplied by a Telco operator
Rationale	No	Transport Infrastructure is relevant for ongoing SG operation, pervasive public networks don’t require high CAPEX and prospect lower OPEX due to shared utilization
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	04/07/2011
Last modified	No	04/07/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	21.EPIC.FINSENY.Component.Telco Infrastructure 2
Name	No	Telco Infrastructure 2
Goal	No	The Communication Technology (CT) layer requires utilization of any useful link available under disturbed operating conditions. This may be supplied by a Telco operator.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	These communication technologies may be utilized: - LTE/4G and UMTS/3G (e.g. for regular operation), - 2G/GPRS – low speed, - WiFi Internet access via Hotspots, - Satellite Links - Direct Ethernet to connect into public networks - DSL (ADSL) modem connection to public operators via twisted pairs (assuming no local power, but central office DSLAM power back-up)
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The Communication Technology (CT) layer requires utilization of any useful link available under disturbed operating conditions. This may be supplied by a Telco operator.
Rationale	No	Transport Infrastructure is relevant for ongoing SG operation, pervasive public networks don't require high CAPEX and prospect lower OPEX due to shared utilization
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	11/07/2011
Last modified	No	11/07/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	90.EPIC.FINSENY.Component.Local processing and storage
Name	No	Local processing and storage

Goal	No	Data processing and storage requirements are indispensable for any sort of building-level intelligence and so to inform the comsumers about the building status (through a human-machine interface) or to communicate with the grid (through an interoperabilit
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Support for on the fly remote configuration
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Data processing and storage requirements are indispensable for any sort of building-level intelligence and so to inform the comsumers about the building status (through a human-machine interface) or to communicate with the grid (through an interoperabilit
Rationale	No	It is obvious that local persistency is required, coupled with redundant cloud-based persistency to support any ICT-heavy energy efficiency mechanisms. More, services need to access and manage a huge amount of data for each appliance, in the time and for
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	12/09/2011
Last modified	No	12/09/2011

Field	ENUM	Description
ID	No	91.EPIC.FINSENY.Component.Remote processing and storage
Name	No	Remote processing and storage
Goal	No	The platform must offer a way for calculating aggregated consumption, energy-related data and costs for homes and buildings with the same profile. Moreover, the consideration of demand-shaping measures and the implementation of peak-shaving capabilities require the grid administrator to have some sort of further data access. Concretely, it is necessary to maintain information about the contract model of each subscriber, the options available to that model, and the extent to which some of these options have already been used. To correctly anticipate future needs, both current real-time energy demands as well as historical information should be available, on which to base reliable forecasts and ensure the timely initiation of load-shifting measures. Furthermore, and subject to privacy requirements, socio-economic profiles may also need to be available for the various subscribers. Besides the processing, storage and availability capabilities, all this requires the definition of a unified and appropriate data model.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Define logical model for remote data that needs to be stored in the cloud. Allow the logical model to be extensible so as to accommodate future requirements. Main concepts to model: subscriber, contracts, incentives and counter-incentives for the implementation of peak shaving features.
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The platform must offer a way for calculating aggregated consumption, energy-related data and costs for homes and buildings with the same profile. Moreover, the consideration of demand-shaping measures and the implementation of peak-shaving capabilities require the grid administrator to have some sort of further data access. Concretely, it is necessary to maintain information about the contract model of each subscriber, the options available to that model, and the extent to which some of these options have already been used. To correctly anticipate future needs, both current real-time energy demands as well as historical information should be available, on which to base reliable forecasts and ensure the timely initiation of load-shifting measures. Furthermore, and subject to privacy requirements, socio-economic profiles may also need to be available for the various subscribers. Besides the processing, storage and availability capabilities, all this requires the definition of a unified and appropriate data model.
Rationale	No	Useful information for the final user
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	12/09/2011
Last modified	No	12/09/2011

Field	ENUM	Description
ID	No	188.EPIC.FINSENY.Component.Web-Service-enabled technologies for electricity network management
Name	No	Web-Service-enabled technologies for electricity network management
Goal	No	Services for monitoring, supervisory control and operation of electrical networks need to be in place. The network infrastructure should feature open web-service APIs so that electro mobility cloud services and marketplace services can simultaneously query and reserve both network and cloud services without any human intervention.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Reliability, Security
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Services for monitoring, supervisory control and operation of electrical networks need to be in place. The network infrastructure should feature open web-service APIs so that electro mobility cloud services and marketplace services can simultaneously query and reserve both network and cloud services without any human intervention.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	27/07/2011
Last modified	No	27/07/2011

Field	ENUM	Description
ID	No	239.EPIC.FINSENY.Component.Smart Metering
Name	No	Smart Metering
Goal	No	Smart Metering is one of the key functions in Smart Energy Grid scenarios. It allows: all customers to have means to analyze/view the corresponding data in order to be precisely aware of their energy consumption; Grid Users and Grid Operators to actually know close-to-real-time consumption (e.g., to decide on various demand-side and production-management activities) and consequently they are able to know when and how much energy they have to trade in order to improve their business efficiency.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Security
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Smart Metering is one of the key functions in Smart Energy Grid scenarios. It allows: all customers to have means to analyze/view the corresponding data in order to be precisely aware of their energy consumption; Grid Users and Grid Operators to actually know close-to-real-time consumption (e.g., to decide on various demand-side and production-management activities) and consequently they are able to know when and how much energy they have to trade in order to improve their business efficiency.
Rationale	No	The requirement is essential in order to know aggregated view of energy consumption/generation.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	15/09/2011
Last modified	No	15/09/2011

Field	ENUM	Description
ID	No	269.EPIC.FINSENY.Component.Control mechanisms for Smart Homes
Name	No	Control mechanisms for Smart Homes
Goal	No	Standardized mechanisms need to be in place in order to: control the energy consumption and production in Smart Homes from the outside; control intelligent devices and electric vehicles within a Smart Home (Internet of Things domain). These mechanisms include in particular communication interfaces, a protocol for information exchange, network connection for all devices and control mechanisms/information exchange (e.g., balancing signals).
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Security
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Standardized mechanisms need to be in place in order to: control the energy consumption and production in Smart Homes from the outside; control intelligent devices and electric vehicles within a Smart Home (Internet of Things domain). These mechanisms include in particular communication interfaces, a protocol for information exchange, network connection for all devices and control mechanisms/information exchange (e.g., balancing signals).
Rationale	No	This requirement is essential as the scenario can only be facilitated with such mechanisms.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	24/08/2011
Last modified	No	24/08/2011

Field	ENUM	Description
ID	No	284.EPIC.FINSENY.Component.Energy Monitoring
Name	No	Energy Monitoring
Goal	No	Mechanisms for delivering data related to the energy consumption and/or production within a Smart House need to be in place for planning, procuring and selling activities. Besides Smart Meters, devices need to be intelligent and to be able to communicate.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Security
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Mechanisms for delivering data related to the energy consumption and/or production within a Smart House need to be in place for planning, procuring and selling activities. Besides Smart Meters, devices need to be intelligent and to be able to communicate.
Rationale	No	This requirement is essential as the scenario can only be facilitated with energy monitoring.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	24/08/2011
Last modified	No	24/08/2011

Field	ENUM	Description
ID	No	300.EPIC.FINSENY.Component.Efficient and secure service access and provision
Name	No	Efficient and secure service access and provision
Goal	No	The Ability of generating contracts on the fly over the internet will need to be reliable by employing standard protocols and interfaces fro the users. Security access has to be provided also following usual
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	The service will need to follow Web 2.0 guidelines and openness. Mostly Web-based interfacing technologies will be used.
Status	Yes	
MoSCoW priority	Yes	SHOULD
Relative priority	No	SHOULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The Ability of generating contracts on the fly over the internet will need to be releable by employing standard protocols and interfaces fro the users. Security access has to be provided also following usual
Rationale	No	The Requirement is mandatory to be able to provide the service.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	09/09/2011
Last modified	No	09/09/2011

10.5 Security Layer

Field	ENUM	Description
ID	No	45.EPIC.FINSENY.Segurity.Authentication and authorization
Name	No	Authentication and authorization
Goal	No	System components shall uniquely authenticate users and specific components before establishing a connection. The components shall enforce separation of duties through assigned access authorization. The user privileges should be restricted to only those that are required for each person's role (role based access restriction), taking into account emergency cases.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Strong authentication based on asymmetric scheme and credentials, like certificates and corresponding private keys; Simple authentication based on ID and password Secure database Means for RBAC enforcement; Secure key storage
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	System components shall uniquely authenticate users and specific components before establishing a connection. The components shall enforce separation of duties through assigned access authorization. The user privileges should be restricted to only those that are required for each person's role (role based access restriction), taking into account emergency cases.
Rationale	No	Peer authentication is the first step towards a secure session establishment and thus builds the base for secured communication. Moreover, authentication and role association is the basis to ensure, that only authorized personnel is able to perform certain actions requiring a dedicated role level. It includes also cases when cars' users identify themselves to the energy supplier via public charge points. However, an identification of the user by every device in the network may not be feasible. In such cases it is necessary to restrict physical access to devices and assume that physical access implies the right to operate the device under a given set of rules.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	27/06/2011
Last modified	No	27/06/2011

Field	ENUM	Description
ID	No	46.EPIC.FINSENY.Segurity.Data backup and recovery
Name	No	Data backup and recovery
Goal	No	Backups of critical software, applications, and data for all components of the SCADA system should be assured.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Data Synchronization Protection of backups (integrity, in certain cases also confidentiality);
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Backups of critical software, applications, and data for all components of the SCADA system should be assured.
Rationale	No	Backup and (plug & play) recovery is crucial to ensure system availability. This is especially necessary in case of system restarts or replacement of dedicated system parts.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	27/06/2011
Last modified	No	27/06/2011

Field	ENUM	Description
ID	No	47.EPIC.FINSENY.Security.Data confidentiality
Name	No	Data confidentiality
Goal	No	It shall be possible to ensure the confidentiality of the communicated data by cryptographic mechanisms, unless otherwise protected by alternative physical measures.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Key generation Encryption mechanisms
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	It shall be possible to ensure the confidentiality of the communicated data by cryptographic mechanisms, unless otherwise protected by alternative physical measures.
Rationale	No	This requirement relates to the need for confidentiality when information is being transmitted from one entity or a group of entities to another entity or a group of entities as well as locally stored data. The data should be accessible only to authorized users as it is sensitive from a privacy, safety, or economical point of view (e.g. metering, contract, or energy exchange information). The level of data protection may (in some UCs) depend on the location. E.g. data exchanged internally within a building automation network may have lower protection level than the data externally exchanged.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	08/06/2011
Last modified	No	08/06/2011

Field	ENUM	Description
ID	No	48.EPIC.FINSENY.Security.Data integrity
Name	No	Data integrity
Goal	No	It shall be possible to ensure the integrity of the communicated data (during the data transfer as well as stored data) and to verify whether the data hasn't been tampered.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Creating and checking cryptographic checksum Cryptographic linked lists Mechanisms and Protocols supporting Key generation / Key Management; Secure key storage
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	It shall be possible to ensure the integrity of the communicated data (during the data transfer as well as stored data) and to verify whether the data hasn't been tampered.
Rationale	No	Integrity protection when information is being transmitted from one entity or a group of entities to another entity or a group of entities is necessary in order to assure that the data hasn't been altered during transmission. Integrity is needed for the communication of information among SCADA system-RTU-Power equipment, Counter-Measures Hub, or actors like Markets and DSO, as well as e.g. for forecasting of energy demand/production
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	08/06/2011
Last modified	No	08/06/2011

Field	ENUM	Description
ID	No	49.EPIC.FINSENY.Security.Non-repudiation
Name	No	Non-repudiation
Goal	No	It shall be possible to prove that information has been send by a specific source to prevent the sender of information from denying sending it.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Digital signature algorithms (e.g., RSA, ECC based solutions); Hash algorithms (e.g., SHA-1, SHA-256, …); Secure private key storage
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	It shall be possible to prove that information has been send by a specific source to prevent the sender of information from denying sending it.
Rationale	No	Authorization validation for audits for dedicated commands. Firmware updates to ensure data origin. Proof of data exchange between different actors e.g. in billing systems.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	27/06/2011
Last modified	No	27/06/2011

Field	ENUM	Description
ID	No	50.EPIC.FINSENY.Security.System protection against malicious code
Name	No	System protection against malicious code
Goal	No	The smart grid system shall employ malicious code protection mechanism.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Firewalls, Antiviral software Intrusion Protection Systems / Intrusion Prevention Systems
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The smart grid system shall employ malicious code protection mechanism.
Rationale	No	One challenge is that the field deployed devices are typically not suitable for traditional third party malicious code protection mechanisms. This combined with very little or no physical security means that emphasis be placed on the risk associated with these widely dispersed assets. Therefore it should be ensured that no malicious code can pass some security zones (e.g. from the utility's NAN to HAN). Field tools represent potentially high risk also because they may be connected to numerous networks.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	24/06/2011
Last modified	No	24/06/2011

Field	ENUM	Description
ID	No	51.EPIC.FINSENY.Security.Intrusion detection
Name	No	Intrusion detection
Goal	No	The system shall detect the anomalous events (e.g. meter data alerted) within the network boundaries.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Intrusion detection systems
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The system shall detect the anomalous events (e.g. meter data alerted) within the network boundaries.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	08/06/2011
Last modified	No	08/06/2011

Field	ENUM	Description
ID	No	52.EPIC.FINSENY.Security.Denial-of-service protection
Name	No	Denial-of-service protection
Goal	No	The system should restrict the ability of internal or external users to launch denial-of-service attacks against the network components.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Traffic monitoring and filtering
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The system should restrict the ability of internal or external users to launch denial-of-service attacks against the network components.
Rationale	No	As single security product or technology cannot protect an energy network control system, a multiple layer strategy involving two or more different overlapping security mechanisms (defense-in-depth), is advised so that the impact of a failure in any one mechanism is minimized. Except for authentication and authorization other access protection means should be used to monitor potential attacks.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	28/06/2011
Last modified	No	28/06/2011

Field	ENUM	Description
ID	No	53.EPIC.FINSENY.Security.Cryptographic Key Establishment and Management
Name	No	Cryptographic Key Establishment and Management
Goal	No	Cryptographic protection and key management infrastructure shall be selected. The selection should match the value of the information being protected and the protected system operating constraints.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Key generation process Generation algorithms
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Cryptographic protection and key management infrastructure shall be selected. The selection should match the value of the information being protected and the protected system operating constraints.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	29/06/2011
Last modified	No	29/06/2011

Definition of entries for the FI-PPP Backlog

Field	ENUM	Description
ID	No	121.EPIC.FINSENY.Security.Data privacy
Name	No	Data privacy
Goal	No	Stored or processed information while not sensitive is still personal and access to it by unauthorized parties would be construed as a privacy infringement reveling the customers daily habits.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	None
Status	Yes	
MoSCoW priority	Yes	SHOULD
Relative priority	No	SHOULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Stored or processed information while not sensitive is still personal and access to it by unauthorized parties would be construed as a privacy infringement reveling the customers daily habits.
Rationale	No	Information whose processing can reveal daily habits or be used to profile a certain electricity subscriber or identify vacancies is stored in various persistent stores at the building and in the cloud. Security of this information and full auditability o
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	12/09/2011
Last modified	No	12/09/2011

Field	ENUM	Description
ID	No	122.EPIC.FINSENY.Security.Workload profiler
Name	No	Workload profiler
Goal	No	Develops and executes a series of experiments (software simulations) to characterize how much energy capping can be applied to the servers before the performance target is hit.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	To do this requirement, the developers must to perform a series of experiments to characterize how much capping can be applied before the performance target is hit. Afterwards, during normal operations, the applications engineer sets power capping targets
Status	Yes	
MoSCoW priority	Yes	COULD
Relative priority	No	COULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Develops and executes a series of experiments (software simulations) to characterize how much energy capping can be applied to the servers before the performance target is hit.
Rationale	No	This requirement is recommended because it allows to increase the Uninterrupted Power Supplies (UPSs) autonomy in case of blackouts due to fortuitous events or to physical intentional attacks.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	16/09/2011
Last modified	No	16/09/2011

Field	ENUM	Description
ID	No	174.EPIC.FINSENY.Security.Fault detection/monitoring system
Name	No	Fault detection/monitoring system
Goal	No	Faults should be detected as early as possible and communicated to given parties. For that reason security monitoring means should be applied.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Security
Status	Yes	COULD
MoSCoW priority	Yes	COULD
Relative priority	No	
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Faults should be detected as early as possible and communicated to given parties. For that reason security monitoring means should be applied.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Field	ENUM	Description
ID	No	177.EPIC.FINSENY.Security.Secure Software/Firmware Updates
Name	No	Secure Software/Firmware Updates
Goal	No	The system shall ensure software/firmware updates only with integrity protected packages from an authorized source.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Integrity protection and authentication mechanisms, e.g., digital signatures; Secure key storage
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	The system shall ensure software/firmware updates only with integrity protected packages from an authorized source.
Rationale	No	Malicious software/firmware updates may compromise the whole system.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Field	ENUM	Description
ID	No	178.EPIC.FINSENY.Security.Security Management
Name	No	Security Management
Goal	No	Security management policy has to consider all involved cryptographic protection means, including key management infrastructure, certificate management, security policies, addressing both, technical and organizational means.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Key generation process; Key generation algorithms; Certificate and CRL generation; Certificate revocation
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Security management policy has to consider all involved cryptographic protection means, including key management infrastructure, certificate management, security policies, addressing both, technical and organizational means.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Field	ENUM	Description
ID	No	225.EPIC.FINSENY.Security.Logging and Audit
Name	No	Logging and Audit
Goal	No	Logging processes shall be established on devices having appropriate resources. Logging supports security monitoring and auditing.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Generation and storage of log files; Examination of log files; Protection of log files
Status	Yes	
MoSCoW priority	Yes	MUST
Relative priority	No	MUST
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	Logging processes shall be established on devices having appropriate resources. Logging supports security monitoring and auditing.
Rationale	No	
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	22/09/2011
Last modified	No	22/09/2011

Field	ENUM	Description
ID	No	286.EPIC.FINSENY.Security.Rating system
Name	No	Rating system
Goal	No	To enhance the trust between different business actors of the system, a rating system that facilitates a possibly objective assessment of the actors shall be available.
Version	No	1
Source	Yes	FINSENY
Source contact	No	Martin Wagner
Stakeholder	Yes	
Scope	Yes	Robustness
Status	Yes	
MoSCoW priority	Yes	SHOULD
Relative priority	No	SHOULD
Chapter	Yes	
Enabler	No	
Category	Yes	
Description	No	A rating system is available that facilitates a possibly objective assessment of all marketplace actors. This enables the prosumers to consider them prior to transactions in order to enhance the prosumers risk management analysis.
Rationale	No	Without a reliable rating system, the system would hardly work.
Owner	Yes	FINSENY
Owner contact	No	Kolja Eger
Complexity	Yes	
Creation Date	No	24/08/2011
Last modified	No	24/08/2011

11. Annex IV – FINSENY Template description

This annex describes the fields defined in the FINSENY template to describe and detail the identified ICT Requirements. The same template was used for the registration and the consolidation of the requirements.

FINSENY Template

- Id: Identification of the ICT Requirement

  Consolidated: Identification assigned after merging of the requirements received from the WPs for consolidation and follow-up proposes.

  Work Package: Identification assigned to the ICT Requirement once received from the WP's.

- Name: Name given to the requirement by the WPs
- Category: Classification value assigned to the requirement

  Layer: General ICT category assigned

  Original: Category assigned to the requirement by the WP

- Source: Source of the information

  Project: FINSENY

  Work Package: WP number

  #UC: Use Case number

- Short Description: Description of the ICT Requirement
- Estimate Priorities: Priority of the ICT Requirement

  FINSENY: Priority assigned by the FINSENY Project

  FI-WARE: Final Priority assigned by the Architecture Board

- Chapter Introduction: AB requirement
- Features: Scope of the Requirement, the features could be:
- Functional: Functional description of the requirement
- Non-Functional: Non-Functional description of the requirement
- Expected issues: Issues related to de deployment of the ICT requirement
- Reference: Reference information for the ICT requirement
- Agreement: Checkbox to detail the agreement on the subject of the relevance of the ICT Requirement
- Justifications: Additional information to justify the priority of the requirement
- Guidance: Detailed description concerning the development and deployment of the requirement.
- Acceptance Criteria: Conditions to be accomplish
- Other: additional information available