

Grant Agreement No.: 604590  
Instrument: Large scale integrating project (IP)  
Call Identifier: FP7-2012-ICT-FI

# **XIFI**

## **eXperimental Infrastructures for the Future Internet**



## **D1.1: XIFI CORE CONCEPTS, REQUIREMENTS AND ARCHITECTURE DRAFT**

Revision: v.1.1

Work package	WP1
Task	Task T1.1
Due date	31/07/2013
Submission date	31/07/2013
Deliverable lead	CREATE-NET
Version	1.1
Authors	Silvio Cretti (CNET), Federico Facca (CNET), Ivan Biasi (TN), Antonio Fuentes (Red-ES), Thomas Guenther (FhG), Sergio Morant (IMAGIN-LAB), Gemma Power (TSSG), Joe Tynan (TSSG), Brian Pickering (IT-INN), Paul Grace (IT-INN), Joaquin Iranzo (ATOS), Jose Gonzalez (UPM), Alexander Willner (TUB), Matthias Baumgart (DT)
Reviewers	Andrea Manieri (ENG), Gerard Nguengang (THALES)

Abstract	This report provides the initial vision of the technical and operational activities performed in XIFI and includes: XIFI federation concept; framework and process for the management of
----------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	capacity building requests by early trial projects; analysis of the core backbone nodes and requirements for the deployment of core platform on top of them; and draft of architecture of XIFI federated platform.
Keywords	Federated platform, requirements, constraints, survey, architecture, federation models

### Document Revision History

Version	Date	Description of change	List of contributor(s)
V1.0	22.07. 2013	Version ready for internal review	Silvio Cretti (CNET) et al.
V1.1	31.07.2013	Final revision	Silvio Cretti (CNET) et al.

### Disclaimer

The information, documentation and figures available in this deliverable, is written by the XIFI (Experimental Infrastructures for the Future Internet) – project consortium under EC grant agreement FP7-ICT-604590 and does not necessarily reflect the views of the European Commission. The European Commission is not liable for any use that may be made of the information contained herein.

### Copyright notice

© 2013 - 2015 XIFI Consortium

Project co-funded by the European Commission in the 7 <sup>th</sup> Framework Programme (2007-2013)			
Nature of the deliverable:		R	
Dissemination Level			
PU	Public		<input checked="" type="checkbox"/>
PP	Restricted to other programme participants (including the Commission Services)		
RE	Restricted to bodies determined by the XIFI project		
CO	Confidential toXIFI project and Commission Services		

## EXECUTIVE SUMMARY

---

This document provides an overview of the XIFI platform describing the vision and objectives, the core concepts and a methodology for gathering and managing requirements and constraints. Using this methodology, a first set of requirements from Use Case projects has been collected and analysed; moreover the five core infrastructure nodes have been described trying to understand possible constraints posed to the XIFI federation. From all the material collected, a set of usage scenarios has been developed for the main situations that can happen in XIFI. Finally a first draft of the XIFI architecture together with a description of the main architectural components has been derived as the main result of this deliverable.

## TABLE OF CONTENTS

<b>EXECUTIVE SUMMARY .....</b>	<b>2</b>
<b>TABLE OF CONTENTS .....</b>	<b>3</b>
<b>ABBREVIATIONS.....</b>	<b>6</b>
1.1 A visual map of XIFI main building blocks (you are here!).....	8
1.2 Scope .....	9
1.3 Document Convention .....	9
1.4 Intended Audience and Reading Suggestions .....	9
2.1 What is an infrastructure according to XIFI .....	11
2.2 XIFI and stakeholders .....	12
2.3 XIFI offer to developers and infrastructure owners.....	13
2.4 XIFI Design Principles.....	13
3.1 XIFI vision .....	16
3.2 From XIFI Stakeholders to Roles .....	16
3.3 How to collect requirements from the stakeholders - The framework.....	17
3.4 How to collect requirements from the stakeholders - The process .....	17
3.4.1 Process for the collection of requirements and expectations from UC projects .....	17
3.4.2 Process for the collection of user requirements and expectations from infrastructure owners: 21	
3.4.3 Process for the collection of FI-WARE requirements: .....	23
3.4.4 Process for the collection of internal requirements:.....	23
4.1 FINESCE (Future InternEtSmart Utility ServiCEs) .....	25
4.1.1 Description .....	25
4.1.2 Summary of information .....	25
4.1.3 Preliminary analysis .....	26
4.2 FIspace (Future Internet Business Collaboration Networks in Agri-Food, Transport and Logistics) .....	26
4.2.1 Description .....	26
4.2.2 Summary of information .....	27
4.2.3 Preliminary analysis .....	28
4.3 FI-CONTENT 2 .....	28
4.3.1 Description .....	28
4.3.2 Summary of information .....	28
4.3.3 Preliminary analysis .....	29

4.4	FITMAN (Future Internet Technologies for MANufacturing industries) .....	30
4.4.1	Description .....	30
4.4.2	Summary of information .....	30
4.4.3	Preliminary analysis .....	31
4.5	FI-STAR (Future Internet Social and Technological Alignment Research).....	31
4.5.1	Description .....	31
4.5.2	Summary of information .....	31
4.5.3	Preliminary analysis .....	32
5.1	Sevilla Node Hardware .....	33
5.2	Trento Node .....	34
5.3	Berlin Node .....	36
5.4	Britanny Node (Lannion) .....	38
5.5	Waterford Node.....	40
5.6	Summary of XIFI Nodes Features .....	42
6.1	An infrastructure owner wants to join the XIFI Federation .....	44
6.2	A UC project wants to setup and use an experimentation environment .....	47
6.3	In order to set-up a cloud infrastructure (non federated with XIFI), XIFI services are used.	50
6.4	An end-user of the Federation requests support and help .....	52
6.5	Management of an Infrastructure (Network and Data Center) .....	54
7.1	Technical Architecture .....	56
7.1.1	Overview .....	56
7.1.2	Minimal network and capacity requirements for each node .....	58
7.1.3	FI-WARE Cloud Hosting Main Constraints .....	59
7.1.4	XIFI Logical Architecture .....	59
7.1.5	Marketplace .....	61
7.1.6	Resource Catalogue.....	62
7.1.7	Recommendation Tool .....	63
7.1.8	Interoperability Tools.....	64
7.1.9	Infrastructure Toolbox .....	65
7.1.10	Federation Service and Resource Manager .....	66
7.1.11	PaaS Manager.....	67
7.1.12	Federated Security and Security Dashboard .....	68
7.1.13	Federation Monitoring .....	69
7.1.14	SLA Management .....	70
7.1.15	HelpDesk .....	71



7.2	Federation Models.....	71
7.2.1	Requirements.....	73
<b>REFERENCES .....</b>		<b>77</b>

## ABBREVIATIONS

---

<b>UC</b>	Use Case
<b>GE</b>	Generic Enabler
<b>SE</b>	Specific Enabler
<b>FI-PPP</b>	Future-Internet Private Public Partnership
<b>IaaS</b>	Infrastructure as a Service
<b>PaaS</b>	Platform as a Service
<b>SaaS</b>	Software as a Service
<b>SMEs</b>	Small and Medium Enterprises
<b>FMC</b>	Fundamental Modelling Concepts
<b>WP</b>	Work Package
<b>QoS</b>	Quality of Service
<b>FI</b>	Future Internet

# 1 INTRODUCTION

XIFI platform aims to be the community cloud<sup>1</sup> for European FI-PPP developers enabled by advanced FI infrastructure in Europe. The FI-PPP (<http://www.fi-ppp.eu>) is an ambitious programme by the European Commission part of the 7<sup>th</sup> Framework Programme aiming at exploring the potential of a common platform for Future Internet technologies to establish new business ecosystems. XIFI, through this community cloud, will provide a market place to access: i) the web-based services offered by FI-PPP (i.e. the Generic Enablers developed by FI-WARE – <http://www.fi-ware.eu/> - and the Specific Enablers provided by Use Case Trials), ii) advanced Future Internet infrastructures that provide capacities, and iii) data to empower the applications developed by early adopters of FI-PPP technologies.

XIFI, as part of the overall vision of FI-PPP and following the principle “eat your own dog food”, is based on FI-PPP technologies delivered by FI-WARE (the so called Generic Enablers). As such, not only XIFI provides FI-PPP technologies to developers that are then able to validate them through their applications (whether they are part of Large Trials or they will be part of Phase III SMEs and web entrepreneurs), it is itself an adopter of FI-PPP technologies. XIFI, through FI-WARE Generic Enablers (in particular the ones part of Cloud Chapter[6]) and through the implementation of new components aiming at providing the glue of the federation, deploys a community cloud that federates different infrastructures across Europe (composed of a data centre and potentially additional advanced infrastructural services such as sensor networks and wireless antenna).

This document is the first of a series that provides insights and guidelines over XIFI platform and services: from requirements of the different stakeholders, their analysis, to the general architecture of the system, going from the hardware (i.e. network and servers) to the software stack and procedures associated. XIFI is a complex system (made of software, physical appliances, procedures and business models) as such it is composed by different macro-blocks that are orchestrated together. This document - and the following updates resulting from activities in T1.2 and T1.3 - is acting as the director of the orchestra: it defines where all the members of the orchestra are sitting on the stage and direct them to achieve a single harmonious execution. This document does not provide single detailed specifications of the different components; it rather provides a framework and guidelines for the different parts of the XIFI system. In the end also, a director of an orchestra coordinates the execution of the music, but leaves the single members of the orchestra to make their performance following the indication of the director.

This deliverable intends to be the first document that parties interested into learning more about XIFI platform and services will read. This gives also the opportunity of “introducing the components of the orchestra” and helping the reader to understand where the different instruments are located on the stage and what he could expect from the different instruments. In the following section, the authors of this document (in the following only “the authors”) will introduce a map of XIFI system and services that allows the readers to orientate across the different building blocks of XIFI. The same map will be available in all XIFI technical related deliverables so as to provide a common feeling to the reader. The authors plan as well to adopt the same principle to guide external stakeholders across the different public documents that will be exposed in the XIFI wiki (<http://wiki.fi-xifi.eu>). It is worth mentioning, in relation to the project wiki, that while this is a static document, the wiki is a live entity and represents the “working” documentation where all the latest evolutions of requirements, derived

---

<sup>1</sup>“Community cloud”. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises”[2].

<sup>2</sup> In Cloud environments based on the high-availability principle, traditional backup services offered by data centers are not



scenarios and architecture are available.

## 1.1 A visual map of XIFI main building blocks (you are here!)

XIFI offers a marketplace to European large-scale trial developers to access FI-PPP technologies and Future Internet infrastructures. The marketplace provides access to Generic Enablers developed in FI-WARE (the horizontal platform), and potentially (to be checked when they will be provided) to the Specific Enablers developed by Use Case projects (the vertical platforms), through a highly available and reliable “federation” of infrastructures. To complement and support the above-mentioned technologies (GEs and SEs), XIFI leverages on FI infrastructures with different characteristics (e.g. in terms of location, user community, quality of service, special hardware).

XIFI aims at illustrating the potential of such marketplace through different showcases that will act as demonstrators of XIFI offer. For example, one of our showcases will illustrate how developers can take advantage of XIFI multi-site infrastructure to build distributed applications with high-availability set-up and QoS controlled across the different used sites.

XIFI offer comprises two main parts: **the platform**, i.e. the “virtual” market place that allows end-users to browse through, configure and access enablers and infrastructures in preparation for their experimentations and **the operational services**, i.e. the set of activities that go around the platform to provide a comprehensive “package” to XIFI end-users. The operational services and the platform go beyond pure technical considerations: they offer a summary vision of technical and business aspects that constitute the XIFI offering.

The **XIFI platform** is conceived with the context of the community cloud deployment model, and offers all the three traditional services models of cloud platforms: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [2]. The XIFI platform is composed of different elements, such as:

- **User Interfaces** comprising tools for browsing, discovering, recommending, configuring, allocating and deploying resources; such interfaces provides as well means to interact with operational services provided by infrastructure owners, such as developers support and SLA management;
- **Federated Cloud and Service Management** for the aggregation of different resources available through the federation, the shared security and identity management across the federation, the software automation for the installation of new nodes and new services on top of nodes;
- **Dynamic Network Management** to support connectivity configuration across federation nodes at the level of single services, fulfilling changing user demand;
- **Resource Monitoring** that supports the active and passive collection of data from physical and virtual sources, providing the capacity to gain access to meaningful information on infrastructure and service availability;

The **XIFI operational services** are a set of fundamental services to support the management of the XIFI platform as well as address the needs of different actors, i.e. infrastructures and application developers. Most of these services are governed by protocols and procedures to ensure the operational continuity of XIFI platform. Such operational activities cover management of the nodes – in particular Level 1 and Level 2 support to developers–, support to infrastructure owners in deployment and maintenance of the platform (with special focus on new infrastructures joining XIFI during its second year) and training for developers and infrastructures owners (it will be built exploiting the showcases and referring to the documentation available from the technical activities over the project).

XIFI building blocks are showed in Figure 1. In this deliverable the authors will introduce general

aspects related to the XIFI Platform and XIFI Services.

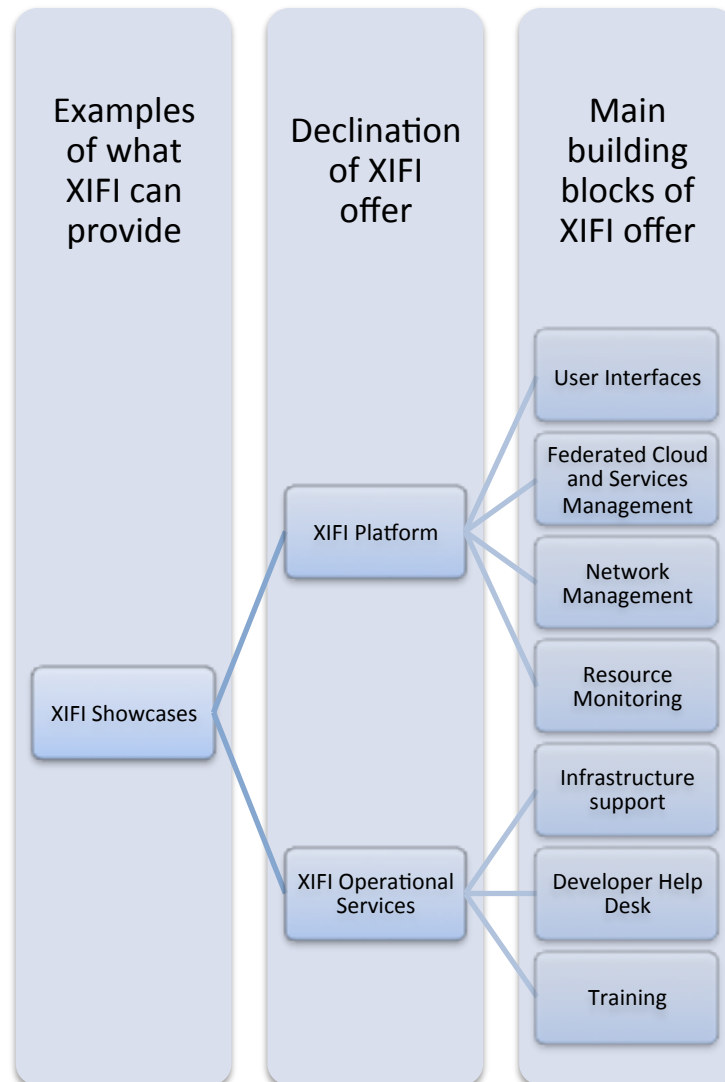


Figure 1. Visual Map of XIFI main building blocks.

## 1.2 Scope

This deliverable focuses on the definition of a common vision and a first set of requirements, constraints and scenarios for XIFI. Using a simple methodology for gathering requirements and constraints, a description of the core nodes and of the Use Case projects is provided. From here, some main usage scenarios have been developed and a first draft of the XIFI architecture derived.

## 1.3 Document Convention

The formatting of the document is compliant with the deliverable template provided by the XIFI project. No other specific convention has been applied.

## 1.4 Intended Audience and Reading Suggestions

The intended audience of this document comprises:

- XIFI partners involved in technical activities so to have a first overview of the concepts, requirements and architecture of the XIFI federation. This overview provides a common and shared starting point to be further developed and detailed inside each technical work package.
- All the XIFI partners in general in order to have a common understanding of the objective of the XIFI project.
- Third party stakeholders like Use Case projects, FI-WARE or in general any IT professional in order to have a clear understanding of the XIFI vision and to provide feedback or suggestions.

The document is divided into the following sections:

- **Section 1** introduces the objectives and scope of the document.
- **Section 2** describes the core concepts beyond XIFI project.
- **Section 3** describes the methodology, process and tools for handling requirements and constraints.
- **Section 4** presents a first analysis of the UC requirements.
- **Section 5** gives a description of the five core backbone nodes.
- **Section 6** provides some main usage scenarios relevant for XIFI.
- **Section 7** describes a first draft of the XIFI architecture.

## 2 CORE CONCEPTS

In this section the authors highlight some of the main guidelines that should be taken into consideration to drive the building of XIFI.

- **XIFI as a community cloud:** XIFI is a federation of resources offered to the FI-PPP developer community by FI infrastructures. FI-PPP developers themselves may contribute to the community cloud by offering additional hardware capacity (under their own control or open to other PPP participants) and their own services (the so called Specific Enablers).
- **XIFI as showcase for promotion of FI-PPP technologies for developers:** XIFI is the natural showcase to promote FI-PPP results by hosting Generic Enablers, Specific Enablers and end user applications build on top of them, by interconnecting data and advanced services offered by FI infrastructures.
- **XIFI as opportunity for FI infrastructures to attract new communities of developers through FI-PPP services:** XIFI aims at identifying, within the project lifetime, ways to ensure its sustainability. The natural way is to proof to infrastructure owners that, keeping alive the community cloud, will allow them to attract communities of developers beyond what they achieved so far. Of course this has several implications related to FI-PPP IPR handling that will be analysed within the XIFI project.
- **XIFI as validation and test of FI-WARE technologies in the field of Cloud Computing:** XIFI can be regarded as an horizontal use case project that leverage on FI-WARE Generic Enablers to show how to build a largely distributed and federated cloud platform that offer FI-PPP technologies to developers. In this sense, it is very important to collaborate with FI-WARE (and the upcoming Technical Foundation project) to define our fine-grained architecture and to provide requirements back to FI-WARE.
- **XIFI as a flexible platform:** the need to integrate and federate different existing infrastructures, demands for ability to tackle different needs raised by infrastructures for their integration, both at technical level, operational level and business level. The flexibility regards also the capacity: for example at the moment it is very difficult to forecast the needed resources (e.g. CPU cores, RAM, storage, network bandwidth) and XIFI should be ready to scale-up (this means also that software and hardware architecture should support that) with the growth of resource demands.

### 2.1 What is an infrastructure according to XIFI

The authors used and will use the term infrastructure (and node as synonym) in different parts of this document and of XIFI documentation. Thus it is important to define what an infrastructure in our context is. **In XIFI an infrastructure is any infrastructure that:**

1. offers capacity to host FI-WARE GEs for building FI applications (**compulsory**). To offer capacity to host FI-WARE GEs, the infrastructure should be able to host the Cloud Hosting GEs offered by FI-WARE through which the other GEs are provisioned. This means, in concrete terms, that the infrastructure should be equipped with a data center
2. offers connectivity to Internet and GEANT network (**compulsory**). Connectivity to Internet allows developers and application end-users to access the services hosted on the infrastructure. This connectivity can be provided through different means (GEANT or other providers). XIFI, to leverage on EU FI facilities and to reduce the cost of connectivity, decided that the backbone network to allow XIFI nodes intra-communication is provided through GEANT

3. offers additional capacities such as: sensing environment, advanced wireless connectivity, smart city datasets (**would like**). Future Internet developers may use such capacities to experiment GEs in real environments and on real data
4. offers services to developers: support, backup, ... (**would like**). Infrastructure may offer additional operational services to enrich their offer. The absence of these services should not be conflicting with operation of XIFI federation<sup>2</sup>
5. offers access to end-user communities (**would like**). Infrastructures may be well connected to communities of end-users that developers can leverage on to test and validate their applications

## 2.2 XIFI and stakeholders

The above discussion revolves around the two main stakeholders of XIFI:

- Future Internet Developers (intended as IT professionals involved in the development of FI applications): application developers that want to leverage on FI-PPP technology platforms to develop innovative applications for so called Future Internet scenarios (e.g. smart mobility, smart energy, smart healthcare, ...).
- Future Internet Infrastructures: infrastructures offering capacity to host Future Internet applications and advanced hardware/services that can be used to support Future Internet application developers. As such Future Internet infrastructures are service hosting providers.

The two stakeholders have different objectives and needs that XIFI should be able to balance in building its offer. Nevertheless, the main objective of FI-PPP programme is to foster large adoption (and validation) of FI-PPP technologies. This requires a critical mass of developers (beyond FI-PPP Large Trials projects) to adopt GEs and SEs to build Future Internet applications. Thus it is crucial for the success of FI-PPP (and of XIFI) to attract as much as possible developers willing to use FI-PPP tools. This clearly gives to FI Developers a privileged position among stakeholders. XIFI should balance these two perspectives (the one of FI Infrastructures and the one of FI Developers) keeping into account as well FI-PPP general objectives.

Other relevant stakeholders in the picture are:

- Future Internet Core Platform developers – which correspond to FI-WARE (and the upcoming Technical Foundation project) developers, and that aim to offer the services (Generic Enablers) part of their platform to the Future Internet Developers.
- Future Internet application sponsors and data providers – that support Future Internet Developers through financial and in-kind resources.
- XIFI Consortium – that is in charge of the different operational and administrative activities to enable the provisioning of XIFI platform.

The stakeholders mentioned above may correspond to one or more role XIFI will take into consideration in the requirements analysis.

---

<sup>2</sup> In Cloud environments based on the high-availability principle, traditional backup services offered by data centers are not more required.

## 2.3 XIFI offer to developers and infrastructure owners

In this section the authors summarize some of the key elements of XIFI offer to developers and infrastructures.

XIFI will offer to developers: *a single entry point to access FI-PPP technologies and underlying advanced Future Internet infrastructures*. Through this entry point:

- The developer will be able to access GEs and SEs deployed on different infrastructures in a transparent way.
- The developer will be able to manage shared and private resources under her/his control.
- The developer will be able to transparently deploy FI-WAREGEs and her/his own SEs.
- The developer will be able to acquire information on the different characteristics of the infrastructures, such as: advanced experimental services (e.g. sensor networks, smart energy grids), SLAs, usage term and conditions.
- The developer will be able to create projects/experiments "encompassing" more than one site (infrastructure) in a transparent way.
- The developer will have a single access point to monitor services he/she is using and platforms he/she deployed.
- The developer will be supported in moving platforms he/she deployed from a location to another.
- The developer will have access to tutorials for deploying FI-WARE GEs and its own SEs.
- The developer will have access to the help desk granting Level 1 and Level 2 support.

XIFI will offer to infrastructure owners: *a single entry point to publish their offer and access services meant for them*. Through the single entry point:

- The infrastructure owners will advertise: advanced experimental services (e.g. sensor networks, smart energy grids), SLAs, usage term and conditions.
- The infrastructure owners will access to tutorials for: joining federation, deploying GEs, connecting GEs with their advances capabilities (e.g. sensor networks).
- The infrastructure owners will access to the help desk granting Level 1 and Level 2 support for federation services and the installation process.
- The infrastructure owners will deploy GEs to be made available in their datacenter.

## 2.4 XIFI Design Principles

In this section the authors highlight the most relevant design principles that have been followed in the definition of XIFI architecture and that should drive as well definition of single components of XIFI described in other technical deliverables. XIFI architecture defines a community cloud platform and as such it should adhere to canonical cloud computing design principles [2] and heterogeneous cloud deployment best practises [3]:

- On-demand self service [2]. "A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider"
- Broad network access [2]. "Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations)".
- Resource pooling [2]. "The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the

exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth”.

- Rapid elasticity [2]. “Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time”.
- Measured service [2]. “Cloud systems automatically control and optimize resource usage by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service”
- User centric [3]. Well-designed services and user interfaces are key to deliver best user experience that will facilitate adoption of cloud services.
- Simplicity [3]. The adoption of complex solutions may impact delivery time and the service quality. Dealing with heterogeneous environments may require complex solutions to automate some of the processes. Some processes may be kept to a manual mode in an initial phase for time-to-market, rather than designing with full functionality and for all IT services.
- Reuse [3]. Cloud computing is nowadays a well-established field where a plethora of solutions are available off the shelves to be deployed to support the creation of cloud based infrastructures. Such solutions should be reused as much as possible to allow for a fast kick-start of cloud provisioning activities, unless there are strong reasons to develop a new solution. Within XIFI, we will aim at adoption of FI-PPP technologies to achieve our architecture and to reuse, where needed, complementary Open Source software and Open Standards. XIFI when extending software to align them with its requirements will contribute back to the communities that originated adopted software.
- Service dependability [4]. Dependability is a fundamental characteristic of cloud computing platforms. Service availability is one of the key attributes for a service to be defined dependable. Service availability requires dealing with issues such as no single point of failure and scalability/elasticity mentioned above. While some of these features are not dependant on the provisioning platform, but rather on the services developed on top of the platform, in the design of Cloud provisioning platform service availability should be carefully planned also taking into consideration derived costs [3]. XIFI architecture aims at delivery dependable services, with focus on availability, reliability, safety and transparency<sup>3</sup> attributes [4]. Services available in the single XIFI nodes, should be available regardless the availability of other nodes. Highly availability and reliability should be provided as well for management tools provided by XIFI platform. Integrity, maintainability and confidentiality should be guaranteed by the reuse of dependable cloud tools.
- Flexibility. The requirements that XIFI will face may change over the time, as such XIFI architecture should be designed for adapting to new requirements. In this sense modularity and service orientation are fundamental principles to be considered to design XIFI architecture.
- Compatibility. XIFI aims at bringing on board as nodes existing Future Internet infrastructures,

---

<sup>3</sup> Transparency, as the capability of inspect a service so as that QoS can be observed and validated is strictly related to the “Measured Service” principle.



as such it is important that the design of XIFI architecture keeps into consideration the continuity of their operational and business activities and that allows for integration of XIFI architecture on top of existing tools adopted by infrastructures (where this does not conflict with FI-PPP technology centric principle).



### 3 FRAMEWORK, PROCESS AND TOOLS FOR HANDLING REQUIREMENTS AND CONSTRAINTS

In order to build a framework for handling the XIFI requirements and constraints, the main "objects" of our domain have to be clearly identified:

- the what – i.e. the vision and the objectives
- the who – i.e. the stakeholders
- the how – i.e. how to implement the requirement gathering

Let's consider each of these separately and elaborate a bit on them.

#### 3.1 XIFI vision

As already mentioned, XIFI is the marketplace for accessing FI-PPP technologies and Future Internet infrastructure offer for large trials developers in Europe. Such a sentence reflects two fundamental elements of XIFI offer:

- XIFI will provide Generic Enablers developed in FI-WARE through high-available and reliable "federation" of infrastructures.
- XIFI, in order to support the provisioning of GEs, will leverage on FI infrastructures with different characteristics (e.g. in term of location, user community, quality of service, "special" hardware).

XIFI will guarantee access only to FI-PPP technologies (by which we mean Generic Enablers developed by FI-WARE and its follow-up). Potential competitor cannot be admitted. Still this of course allows for "competitive" implementation of GEs: if a third party develops a GE implementation that respects the GE Open Specifications, then that should be considered part of the FI-PPP ecosystem as well.

XIFI is essentially a community cloud that, besides access to virtualized infrastructure, includes as well services suitable for the development of advanced internet based applications.

#### 3.2 From XIFI Stakeholders to Roles

Following the vision stated in the previous section and the stakeholders listed in 2.2 the following roles can be identified:

- **Application Developers**, that include both Use Case projects and developers that will be involved in FI-PPP Phase III through SMEs and web entrepreneurs;
- **Infrastructure Owners**, that includes both infrastructure owners currently part of XIFI federation and future ones that will be included through the XIFI Open Call process or other means. This role is in charge of providing and operating the hosting infrastructures on top of which applications and GEs are deployed;
- **Generic Enablers Developers**, that includes (but is not limited to) both developers of FI-WARE and of the up-coming Technical Foundation project. In the future new stakeholders can impersonate this role.
- **XIFI Instance Providers**, that is in charge of the different operational and administrative activities to enable the provisioning and the operation of XIFI platform.

Of course each role has his proper objectives and perspectives:

- Application Developers aim at having a high variety and amount of services and resources at

their disposal with high quality of service and performance. Moreover they would like to manage these resources by themselves almost as they would be private resources.

- Infrastructure Owners aim at the integrity and sustainability of their infrastructures and prefer to keep the control of them avoiding the risk of jeopardizing their resources. This is partially in conflict with the objective of the UC developers.
- GE Developers aim at fostering the GEs adoption looking at platforms that are compatible with their installation. This could be partially in conflict with the objectives of infrastructure owners if it is requested a disruptive upgrade in order to host some GEs.
- XIFI Instance Providers aim at improving the XIFI federation and in general fostering the FI-PPP program results attracting more infrastructures and more developers. On the other side XIFI Instance Providers need to avoid jeopardizing the integrity of the XIFI Federation and the respect of the FI-WARE results: this means that not all the infrastructures will be suitable for joining the federation and that not all the requests from the UC projects can be satisfied.

### 3.3 How to collect requirements from the stakeholders - The framework

Defined the roles related to the stakeholders as in the previous section, a method to collect their expectations is needed. This method should be:

- simple enough in order to avoid to annoy the stakeholders (in particular the external ones)
- collaborative so that the stakeholders can improve the information provided in an iterative way.

Bearing in mind these two principles, the following means have been identified in order to collect the expectations from each stakeholder having a role in XIFI:

- online survey for Application Developers (UC projects) and Infrastructure Owners with a XIFI partner as facilitator
- technical working groups with GE Developers (FI-WARE)
- definition of some preliminary showcases for collection of requirements from XIFI Instance Providers (the XIFI Consortium).

Regarding the tools that should be used for supporting the requirement gathering, the following should be taken into account:

- the tool that should be used to launch the survey can be either googleforms and the project wiki for its analysis
- the technical working groups should meet (virtually, i.e. telco) approximately every two weeks and share its results on the project wiki in a collaborative manner
- the showcases and other internal requirements should be defined on the project wiki.

### 3.4 How to collect requirements from the stakeholders - The process

Four different processes, related to the different roles previously identified, can be distinguished. Hereunder a description of each of these processes.

#### 3.4.1 Process for the collection of requirements and expectations from UC projects

As regards to UC projects we identified two main processes: the first one to identify general requirements to XIFI platform in term of services and to XIFI capacity in term of existing nodes; the second one to elicit requirements to additional capacity to be provisioned by XIFI through the Open

Call process.

### Process for the collection of general requirements and expectations from UC projects

1. definition of a survey for collecting UC requirements: all the WP1 partners should collaborate on this item
  - submission of the survey to the FI-PPP Architectural Board for approval
2. designation of a partner that works as facilitator for the UC survey
3. launch of the survey using a tool that allow collaborative editing
4. collection and analysis of the answers by all the partners in WP1 highlighting the main requirements or constraints posed to XIFI: the focus is in particular on the cloud, monitoring and security aspects because these are the foundation for all the others aspects
5. if some answers were not clear, ask the facilitator partner to contact the relevant UC project
6. formalize the results of the analysis in order to use them to drive the definition of some scenarios and of a draft of the XIFI architecture (both business model and technical model)

In a similar way, when UC Projects will deliver their architectures, we will proceed with the analysis of UC requirements that will be considered in D1.2:

1. designation of a partner that works as facilitator for the analysis of UC architecture
2. creation of a collaborative area for the discussion of the UC architecture
3. collection and analysis of requirements raised by UC architectures by all the partners in WP1 highlighting the main requirements or constraints posed to XIFI
4. if some points are not clear, ask the facilitator partner to contact the relevant UC project
5. provide feedbacks to UC project on their architecture so as to maximise advantages from the adoption of XIFI offer

Hereunder is provided the list of the questions included in the UC surveys. The UC survey is split into two parts: one related to the whole UC project and one related to each trial inside the project. The trial survey should be filled by all the trials of a given UC project.

### UC Shared Survey

Question	Answer	Comments
UC coordinator's name		
XIFI contact point's name		
UC architects' names		
Brief UC domain description		
When will be available your first draft of the architecture and service topology?		
Do you plan to use XIFI shared resources to host your platform? If yes, a single instance of the platform or multiple ones?		
Which provisioning model do you envision for the FI-WARE GEs: <ul style="list-style-type: none"> <li>• PaaS</li> <li>• SaaS</li> </ul>		

• both		
What are the FI-WARE GEs “shared” across your trials?		
Do you plan to use any specific PaaS or DevOps tool or you just plan to rely on whatever FI-WARE and XIFI will provide to automatize your platform deployment? If yes which ones?		
Do you plan to use a cloud platform outside XIFI (i.e. not managed by XIFI) and/or to install GEs also on your premises? If yes which ones?		
Any other generic requirement? If yes which ones?		

### *UC Trial Specific Survey*

Question	Answer	Comments
Contact point of the trial		
Please specify the location where your trial will be executed		
Please specify your “favourite” XIFI node (if any): <ul style="list-style-type: none"> <li>Berlin,</li> <li>Waterford,</li> <li>Trento,</li> <li>Britanny,</li> <li>Sevilla.</li> </ul>		
By when will you need to access a production environment for the trial? (testing GEs can still rely on the FI-WARE test-bed till XIFI is ready)		
Please specify your computing and storage needs (capacity requirements)		
Which FI-WARE Generic Enablers do you need? Specify the list in descending priority order, highlighting the ones requested in the first 9-12 months of experimentation		
Is this trial multi-site, ie may need to use different interconnected services from different XIFI nodes? If yes do you have any requirement on bandwidth, latency etc.		
What sort of connectivity do you anticipate requiring? <ul style="list-style-type: none"> <li>we already have an internet access and that is enough</li> <li>we need to upgrade our access to the internet</li> <li>we need static point-to-point ethernet links</li> <li>we need short term dynamic point-to-point links</li> <li>we need 10Gbit/s or greater dedicated links</li> </ul>		
Do you expect to require a static network infrastructure for the length of the project, or to provision new links/remove old links over time?		
How will your equipment connect to the internet? <ul style="list-style-type: none"> <li>with the institution’s addresses</li> <li>request independent connectivity and addresses</li> <li>request independent connectivity and can provide addresses</li> </ul>		

• other (please specify)		
Which locations do you wish to connect to, and how many physical ports do you expect to need at those locations? (Gigabit Ethernet, 10GE, other?)		
Can you provide a physical/logical picture (including geographies) of this trial at an infrastructure level (that is, the physical/logical network, servers and connectivity)?		
Do you have any specific requirement for a given node of the XiFi federation? (non conventional hardware/software)		
Any specific QoS/SLA requirement (e.g.: specific guarantees of the services provided by the nodes)?		
Do you require any other operational service? <ul style="list-style-type: none"> <li>Scalability/Elasticity</li> <li>Backup and Recovery</li> <li>Help Desk</li> <li>Tutoring</li> <li>Authentication</li> <li>Authorization</li> <li>Data encryption/data protection</li> <li>Multi-tenancy</li> <li>Monitoring and logging</li> </ul>		
Any other requirement?		

### The process for the collection of UC requirements for the XIFI Open Call.

The procedure mimics the one described previously for the collection of UC requirements:

1. definition of a survey for collecting UC requirements: all the WP1 partners should collaborate on this item.
2. designation of a partner that works as facilitator for the UC survey.
3. launch of the survey using a tool that allow collaborative editing.
4. collection and analysis of the answers by all the partners in WP1 highlighting the main requirements or constraints posed to XIFI Open Call.
5. if some answers were not clear, ask the facilitator partner to contact the relevant infrastructure owner.
6. formalize the results of the analysis in order to use them to complete the definition of the text of XIFI Open Call.

Hereunder the structure of the survey.

Question	Answer
Which of these “component” are needed by your UC? <ul style="list-style-type: none"> <li>Cloud Computing</li> <li>Sensor Networks</li> <li>Customer Devices</li> </ul>	

<ul style="list-style-type: none"> <li>• Communication Networks (Mobile, WiFi etc.)</li> <li>• Others (please specify)</li> </ul>	
For each of the previous component you chose, please detail you requirements (standard to be supported, particular hardware etc)	
<p>Which operational requirements are needed by your UC?</p> <ul style="list-style-type: none"> <li>• Data protection (please specify the details)</li> <li>• Support time (e.g. 24x7) (please specify the details)</li> <li>• Availability (please specify the details)</li> <li>• Backup services (please specify the details)</li> <li>• Other (please specify)</li> </ul>	
<p>Which of these “business” requirements are needed by your UC?</p> <ul style="list-style-type: none"> <li>• Geo-Localization</li> <li>• Data accessible through the infrastructure (e.g. open data)</li> <li>• Presence of Communities (of users or prosumers)</li> <li>• Target domain related (eHealth, Smart Cities, Smart Grids etc)</li> <li>• Others (please specify)</li> </ul>	

*Note: the deadline for the collection of this input is beyond the date of delivery of this document. These requirements will be documented in the wiki and included in the following D1.2 and in the consolidated version in the annex to the XIFI Open Call text.*

### 3.4.2 Process for the collection of user requirements and expectations from infrastructure owners:

1. definition of a survey for collecting infrastructure requirements and constraints: all the WP1 partners should collaborate on this
2. designation of a partner that works as facilitator for the infrastructure survey
3. launch of the survey using a tool that allow collaborative editing
4. collection and analysis of the answers by all the partners in WP1 highlighting the main requirements or constraints posed to XIFI: the focus is in particular on the cloud, monitoring and security aspects because these are the foundation for all the others aspects.
5. if some answers were not clear, ask the facilitator partner to contact the relevant stakeholder
6. formalize the results of the analysis in order to use them to drive the definition of some scenarios and of the XIFI architecture (both business model and technical model).

Hereunder the structure of the survey.

### Infrastructure Survey

Question	Answer	Comments
What is your infrastructure for?		
Who are its intended users?		
What are its main technical features? <ul style="list-style-type: none"> <li>• Data centre</li> <li>• Backbone network(s)</li> <li>• Wired access network(s)</li> <li>• Wireless access network(s)</li> <li>• Mobile access network(s)</li> <li>• Sensor network(s)</li> <li>• Other (please specify)</li> </ul>		
How heavily utilised are your resources? <ul style="list-style-type: none"> <li>• &lt; 10%</li> <li>• 10% 50%</li> <li>• 50% - 80%</li> <li>• &gt; 80%</li> </ul>		
For the following features that might be provided by the XIFI federation, which statement best matches your needs should you become a member (Must be provided by XIFI, Should be provided by XIFI, Could be provided by XIFI, Would prefer to provide it ourselves, we provide it ourselves and it must be used)? <ul style="list-style-type: none"> <li>• Issuing and managing identity and other attributes to users</li> <li>• Authenticating/verifying user identity and other attributes</li> <li>• Allocating my resources to match user requirements (i.e. a match-making service)</li> <li>• Informing users that my resources match their requirements, but leaving them to contact me to get resources allocated (i.e. a recommendation service)</li> <li>• Monitoring availability of my resources</li> <li>• Negotiating service level agreements with users</li> <li>• Mediating access to my resources once allocated (e.g. by allowing users to send requests indirectly via a XIFI portal or gateway)</li> <li>• Monitoring usage of my resources and generating accounting data (based on SLA terms) for users coming through XIFI</li> <li>• Monitoring the security status of my resources</li> </ul>		
Please indicate any other features not mentioned above for which you have similar constraints		
Please specify the capacity of your infrastructure in terms of cpu, disk, and memory.		
Please briefly describe the network of your infrastructures in terms of connectivity to internet, bandwidth, presence of SDN capable devices etc.		
Do you provide any virtualization support (hypervisor)? If yes, which one?		

Do you provide any IaaS cloud management? If yes, which one?		
Do you provide any PaaS cloud management? If yes, which one?		
Are the components in your infrastructure replaceable if needed (e.g. cloud stack software)? Under which conditions? Please explain.		
Do you provide any "assurance management" (e.g. monitoring, fault, performance, SLA)?		
Which of these security services do you provide (e.g. authentication, authorization, data protection)?		
Could you provide the name and email address of a contact person for this category of questions (Performance Monitoring)?		
Could you indicate the current network monitoring system (if any) and if it is Open Source or proprietary? If it is open source, please indicate the license, e.g. GPL, BSD etc.		
Could you briefly list the main measures/parameters collected for monitoring the network		
Indicate the availability to support other multi-domain monitoring modules (e.g. perfSONAR)		
How can the monitoring data be accessed from an external system?		
Is the monitoring system for servers, services and data centres different to the one indicated above for the network? if yes, please describe your monitoring system hereunder.		
Could you briefly list the measures/parameters collected for monitoring servers, services and data centres?		
Does your infrastructure already make use of FI-WARE GEs (Monitoring GE and DCRM GE) in order to monitor servers, services and data centres?		

### 3.4.3 Process for the collection of FI-WARE requirements:

1. put together a technical team with the needed skill to discuss on cloud, monitor and security aspects and composed by technical persons from XIFI and FI-WARE (XIFI Technical Coordinator, XIFI WPL, FI-WARE Technical Coordinator, FI-WARE Cloud WPL and other FI-WARE technical people if requested)
2. meet periodically finalizing the results obtained on a collaborative platform
3. do homework (on the XIFI side) in order to learn the FI-WARE platform and to improve the XIFI understanding of the FI-WARE platform
4. analyse the results and use them to drive the definition of the XIFI scenarios and the architecture.

### 3.4.4 Process for the collection of internal requirements:

In this first phase of the project, XIFI will concentrate on the internal requirements related to the showcases developed in work package 6. In the following periods, when business models activities covered in work package 8 will be mature enough to provide requirements, we will kick-off also an internal activity to collect their requirements; for now we define only a simplified process.



### Process for the collection of showcases requirements:

1. provide a template to be filled with the description of the showcases (see table below)
2. ask partners involved in WP6 to provide the description of showcases
3. analyse the information obtained in order to drive the definition of the XIFI scenarios and the architecture.

Partner	
Domain	
Relevant XIFI aspects	
Adopted enablers	
Showcase title	
Task assignment	<mention which task your show case is part of: of e.g. 6.1, 6.n.>
Showcase motivation	<three to four sentences>
Showcase usage scenario	<max half a page of text and provide a graphical explanation>
Technical description	<describe how the showcase works in a technical way>
Technical description of components	<FI-WARE Generic Enablers (GE) Self developed parts, specific enablers Other technical aspects XIFI Capacities / Services>
Requirements to nodes / other work-packages within XIFI	
Involved partners and description of their contributions	
Release Plan	

### Process for the collection of other internal (business) requirements:

1. provide a template to be filled with the description of the business use cases
2. ask partners involved in WP8 to provide the description of business use cases
3. analyse the information obtained in order to drive the definition of the XIFI scenarios and the architecture.

*Note: Input from showcases and business models activities are not yet ready to be included in this deliverable. It will be considered in the next phase.*

## 4 PRELIMINARY SURVEY ON UC AND UC REQUIREMENTS

This section describes the results collected through the survey on the five UC projects. Also a first analysis of the data collected is provided.

### 4.1 FINESCE (Future INternEtSmart Utility ServiCEs)

#### 4.1.1 Description

FINESCE will organize and run user trials that range from efficient energy usage in residential and industrial buildings, to developing a new prosumer energy marketplace, building a cross-border private virtual power plant, using electric vehicles as an element of demand response systems, enabling energy providers to move from reactive to pro-active energy network management by providing them with Future Internet ICT, enabling them to better balance volatile solar and wind energy generation with demand for energy. The FINESCE trials will prove the practical applicability of Future Internet technologies and the FI-WARE Generic Enablers to the challenges of the energy sector. FINESCE will develop an active community of innovative SME's, preparing them for the exploitation of the emerging business opportunities in energy, creating jobs, social impact and economic growth. FINESCE builds on and extends the results of the FI-PPP FINSNEY project to realise sustainable real time smart energy services. The consortium includes globally leading energy and ICT operators, manufacturers and service providers and outstanding research organisations and SME's, from 12 countries, contributing directly to tightly focused trials and business innovation. It has the scale and scope to ensure that the FINESCE results drive the FI-WARE and Future Internet success and long-term exploitation internationally. The following primary work areas will be targeted:

- FI providing the sustainable smart city
- Energy eco-system
- FI for end users of energy eco-systems
- FI developing the B2B energy ecosystem
- FI building the Energy Marketplace
- FI in electricity in action.

#### 4.1.2 Summary of information

Below are listed the most relevant details extracted from the survey:

- The information provided is still preliminary. In the next months detailed design for each Trial will be provided.
- FINESCE does plan to use XIFI shared resources but in some cases they plan to use a cloud outside XIFI (sort of private cloud)
- A first preliminary list of FI-WARE GE that FINESCE is going to use is provided hereunder:

<b>IoT Chapter</b>	<ul style="list-style-type: none"> <li>• Communications</li> <li>• Resources Management</li> </ul>
<b>Apps Chapter</b>	<ul style="list-style-type: none"> <li>• Repository</li> <li>• Marketplace</li> <li>• Business Models</li> </ul>
<b>Data Chapter</b>	<ul style="list-style-type: none"> <li>• Publish/Subscribe Broker</li> <li>• Complex Event Processing</li> <li>• BigData Analysis</li> </ul>

	<ul style="list-style-type: none"> <li>• Unstructured data analysis</li> <li>• Mobility Analysis</li> <li>• Real-time Recommendations</li> <li>• Web Behaviour Analysis</li> </ul>
<b>Security Chapter</b>	<ul style="list-style-type: none"> <li>• Data Handling GE</li> <li>• DB Anonymizer GE</li> <li>• Identity Management GCP</li> <li>• Identity Management One</li> <li>• Security Monitoring GE</li> </ul>
<b>Cloud Chapter</b>	<ul style="list-style-type: none"> <li>• IaaS DataCenter Resource Management</li> <li>• IaaS Service Management</li> <li>• PaaS Management</li> <li>• Object Storage</li> <li>• IaaS Cloud-edge Resource</li> <li>• Resource Monitoring</li> </ul>
<b>Interface to Networks</b>	<ul style="list-style-type: none"> <li>• Connected Devices Interfaces (CDI)</li> <li>• Cloud Edge</li> <li>• Network Information Control (NetIC)</li> <li>• Service, Capability, Connectivity and Control (S3C)</li> </ul>

- Basically all the Trials request scalability, authentication/authorization and monitoring services

#### 4.1.3 Preliminary analysis

After reviewing the information provided by the FINESCE consortia in the survey, the main conclusion obtained is that FINESCE is planning to leverage the XIFI federated facilities. They are still in the complex process of evaluating the GEs that can be offered in production mode by XIFI, as well as trying to determine how to make the best use of the XIFI Platform for the FINESCE use case. In some cases a sort of "private" cloud will be needed: this finding has conducted to the elaboration of the scenario described in 6.3.

## 4.2 FIspace (Future Internet Business Collaboration Networks in Agri-Food, Transport and Logistics)

### 4.2.1 Description

The main objective of the FIspace project is to develop, validate, and establish a future business collaboration platform that facilitates information exchange, communication, and coordination among business partners. It prepares the way for fundamental changes in how collaborative business networks and the involved stakeholders work in the future. This project will leverage Future Internet technologies developed in the FI PPP, and be implemented in an open manner so that other FI PPP projects, as well as external IT providers and interested users, can easily use, test, and exploit its features and services and contribute to its expansion and establishment.

FIspace will be a value added *Collaboration Space* that enables actors operating in *Collaborative Business Networks* (e.g. enterprises of all sizes, authorities, public and private service providers) in the

Agri-Food and Transport and Logistics application domains to seamlessly interact, communicate, and coordinate activities with business partners and to easily create and act in open and dynamic networks of connected businesses.

In total, the project aims at establishing 8 use case trials, organized along 3 themes:

- **Farming in the Cloud** addresses food production issues at the farm level
- **Intelligent Perishable Goods Logistics** addresses monitoring and environmental management issues of perishable goods
- **Smart Distribution and Consumption** is about helping consumers to obtain better information on the goods they purchase, and producers to better control the flow of their goods to the consumer

#### 4.2.2 Summary of information

Below are listed the most relevant details extracted from the survey “UC Shared Survey” (information referring to the “UC Trial Specific Survey” was not provided):

- The information is very preliminary and will be better detailed in the next months
- It appears that FIspace does not plan to use XIFI shared resources. Nevertheless probably they will leverage on some services provided by XIFI in a dedicated/private environment (sort of private cloud).
- They are considering to use the following FI-WARE GEs functionalities:

<b>Data Chapter</b>	<ul style="list-style-type: none"> <li>• Complex Event Processing (CEP)</li> <li>• Publish/Subscribe Broker</li> <li>• Middleware</li> </ul>
<b>Apps Chapter</b>	<ul style="list-style-type: none"> <li>• Service Description Repository</li> <li>• Service Registry</li> <li>• Marketplace (part of Business Framework)</li> <li>• Store (part of Business Framework)</li> <li>• Revenue Sharing (part of Business Framework)</li> <li>• Application Mashup</li> <li>• Mediator</li> </ul>
<b>IoT Chapter</b>	<ul style="list-style-type: none"> <li>• (Backend) Configuration Management</li> <li>• (Backend) IoT Broker</li> <li>• (Backend) Device Management</li> <li>• (Gateway) Data Handling</li> <li>• (Gateway) Device Management</li> </ul>
<b>Cloud Chapter</b>	<ul style="list-style-type: none"> <li>• IaaS DataCenter Resource Management</li> <li>• IaaS Service Management</li> <li>• PaaS Management</li> </ul>
<b>Security Chapter</b>	<ul style="list-style-type: none"> <li>• Security Monitoring</li> <li>• Identity Management</li> <li>• Privacy</li> <li>• Access Control</li> <li>• Data Handling</li> <li>• Secure Storage</li> </ul>

	<ul style="list-style-type: none"> <li>• Context-based Security &amp; Compliance</li> <li>• DB Anonymizer (Opt)</li> <li>• Malware Detection Service (Opt)</li> <li>• Android Flow Monitoring (Opt)</li> <li>• Content-based Security (Opt)</li> </ul>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### 4.2.3 Preliminary analysis

After discussing with the FIspace contact person and reviewing the information filled in the survey “UC Shared Survey”, the main conclusion obtained is that FIspace is not considering leveraging the XIFI federated facilities. The domain specific capabilities and critical GEs that FIspace needs to use are planned to be hosted within a FIspace’s proprietary infrastructure. Nevertheless they are committed at least to evaluate the use of the services and facilities that will be offered in production mode by XIFI. In case these services would match the FIspace requirements, a scenario like the one described in 6.3 would be taken into consideration.

## 4.3 FI-CONTENT 2

### 4.3.1 Description

FI-Content 2 is the project which follows up and leverages knowledge of FI-Content from Phase 1 of the FI PPP. This project aims at establishing the foundation of a European infrastructure for promoting and testing novel uses of audio-visual (AV) content on connected devices and will develop and deploy advanced platforms for Social Connected TV, Mobile Smart City services, and Gaming/ Virtual worlds. To assess the approach and improve these platforms, user communities in 6 European locations will be activated for living lab and field trials. The project is strongly supported by local stakeholders (regional authorities, associations, educational organizations, user groups) who will participate in the project via “User Advisory Boards”. The technical capabilities of the platforms will be validated and improved by integrating new - content usage driven - partners recruited via the open call planned early in the project. The FI-Content 2 partnership is a balanced group of large industrial, Content and Media companies, technology suppliers, Telecommunications/Internet access operators, Living labs and Academic institutions. It harnesses the power and excitement of content on the new Internet to drive European innovation, content creation and distribution to enrich the lives of all Europeans.

FI-Content 2 will promote and experiment novel usages of CONTENT on connected devices through 3 different uses cases, each aiming at being a platform open to third party developers:

- Social Connected TV: personalized search and recommendation of broadcast and video on demand content using smart TVs, tablets or browsers, with multi screens interaction
- Smart City Guide: allow users and communities to combine, organize and visualize live Open Data, User Generated Content, user experience and feedback, and editorial content for personalized and contextualized media services aiming at discovering places, people, venues and live events.
- Gaming/ Virtual worlds: enable strong mix of real life and Internet experience, making virtual 3D environments immersive and real, and enabling gamification of Internet applications.

### 4.3.2 Summary of information

The most relevant outcomes from the surveys provided by the UC are:

- FI-Content 2 is interested in both SaaS and PaaS provisioning models, depending on the specific case

- The project intends to leverage XIFI shared resources to host multiple instances of their platform
- It is also required to use a cloud platform outside XIFI for different reasons:
  - A platform is needed since the beginning of the project
  - Partners are already using their own clouds
  - Low latency necessary in locations where no XIFI nodes are available
  - Necessity of Content Delivery Networks
- They are using the open-source CloudFoundry as PaaS Manager
- They are considering these FI-WARE GEs functionalities:

<b>Cloud Chapter</b>	<ul style="list-style-type: none"> <li>• Allocation of single VMs (image instances)</li> <li>• Management of Blueprints</li> <li>• Deployment of SW on single VMs</li> <li>• Allocation of Object Storage</li> <li>• Edgelets Management</li> </ul>
<b>Data Chapter</b>	<ul style="list-style-type: none"> <li>• Complex Event Processing (CEP)</li> <li>• BigData Analysis</li> <li>• Location</li> <li>• Middleware</li> </ul>
<b>Apps Chapter</b>	<ul style="list-style-type: none"> <li>• Marketplace (part of Business Framework)</li> <li>• Service Composition</li> <li>• Service Mashup</li> </ul>
<b>Cloud Chapter</b>	<ul style="list-style-type: none"> <li>• IaaS DataCenter Resource Management</li> <li>• IaaS Service Management</li> <li>• Object Storage</li> <li>• Monitoring</li> </ul>
<b>Security Chapter</b>	<ul style="list-style-type: none"> <li>• Security Monitoring</li> <li>• Identity Management</li> <li>• Access Control</li> </ul>

- Basically all the Trials request scalability, authentication/authorization, monitoring and all the other operational services that XIFI can provide

#### 4.3.3 Preliminary analysis

The good level of information and specification gives us a clear idea of the project's context and what they expect from XIFI. The main conclusion obtained from the assessment is that they are open to use the XIFI offer. Apart from the fact that they require the use of a proprietary cloud platform for some specific cases (e.g. for fulfilling the needs of a Content Delivery Network), FI-Content 2 is willing to leverage XIFI shared resources, both the SaaS and the PaaS provisioning models. In the future XIFI should better analyse the decision of FI-Content 2 to use CloudFoundry as a PaaS Manager tool: the reason of this decision should be better understood and it should be clarified if they can migrate to use the FI-WARE PaaS Manager GE instead.

## 4.4 FITMAN (Future Internet Technologies for MANufacturing industries)

### 4.4.1 Description

FITMAN (Future Internet Technologies for MANufacturing industries) aims to provide the FI-PPP with a set of 11 industry-led use case trials in the Smart, Digital and Virtual Factories of the Future Internet domains. It will test and assess the suitability, openness and flexibility of FI-WARE Generic Enablers, contributing to the social-technological-economical-environmental-political sustainability of EU Manufacturing Industries.

FITMAN is currently working to define the requirements of the different trials, identifying the FIWARE GE that they want to use, and defining their architecture. So, the information provided are still preliminary and minimal. More input will be provided to XIFI in the next months.

### 4.4.2 Summary of information

The summary of the current available information is below:

- They have intention to use XIFI shared resources, however each trial has a very different scope, varying requirements, constraints, features and services so the usage of XIFI should be better analysed. Nevertheless they are considering using a cloud platform outside XIFI, through a core FITMAN IT partner that will play the role of “FI-WARE-Platform Provider”. They also remarked that one trial has serious concerns about data confidentiality and their implications.
- They want to use both PaaS and SaaS provisioning model.
- They are working to define the GE list that will be used, however a preliminary GE list has been provided. They plan to experiment with these GEs and consider them based on results.

<b>Cloud Chapter</b>	<ul style="list-style-type: none"> <li>• Allocation of single VMs</li> <li>• Management of Blueprints</li> <li>• Allocation of Object Storage</li> <li>• Cloud Proxy</li> </ul>
<b>Data Chapter</b>	<ul style="list-style-type: none"> <li>• Complex Event Processing</li> <li>• Publish/Subscribe Broker</li> <li>• Publish/Subscribe Broker</li> <li>• BigData Analysis</li> <li>• Semantic Application Support</li> </ul>
<b>Apps Chapter</b>	<ul style="list-style-type: none"> <li>• Service Description Repository</li> <li>• Service Registry</li> <li>• Marketplace (part of Business Framework)</li> <li>• Store (part of Business Framework)</li> <li>• Light Semantic Composition</li> <li>• Application Mashup</li> <li>• Mediator</li> </ul>
<b>IoT Chapter</b>	<ul style="list-style-type: none"> <li>• (Backend) IoT Broker</li> <li>• (Gateway) Data Handling</li> <li>• (Gateway) Protocol Adapter</li> <li>• (Gateway) Device Management</li> </ul>



<b>Security Chapter</b>	<ul style="list-style-type: none"> <li>• Security Monitoring</li> <li>• Identity Management</li> </ul>
-------------------------	--------------------------------------------------------------------------------------------------------

- In general the trials request operation services like scalability, authorization/authentication and monitoring/logging.

#### 4.4.3 Preliminary analysis

In spite the information gathered is very preliminary, we can provide a first analysis of it.

It appears that they want to use the XIFI shared resources, however they are also considering to use an alternative provider (which is part of the FITMAN consortium). The authors understood that they have constraints about the data confidentiality (at least in one trial). Moreover it seems that they want to use the XIFI operational services so that the authors could foresee a model where these services are provided by XIFI also on infrastructures not federated with XIFI itself (see the scenario depicted in section 6.3).

### 4.5 FI-STAR (Future Internet Social and Technological Alignment Research)

#### 4.5.1 Description

The FI-STAR project aims to fund early trials in the Health Care domain building on Future Internet technology leveraging the outcomes of Future Internet Private-Public Partnership (FI-PPP) Phase 1. In order to meet the requirements of the global health industry, FI-STAR will use a fundamentally different, "reverse" cloud approach: it will bring the software to the data, rather than the data to the software. Thus, it will create a robust framework based of the "software-to-data" paradigm. The main challenge for FI-STAR is that the data (personal health data - which in some jurisdictions are regarded as "sensitive data") may not leave the end-user's private cloud.

There are planned to be seven early trials across Europe, serving more than 4 million people. Through these trials the core FI-PPP platform concept will be validated by using GEs to build the operational framework and the introduction of ultra-light interactive applications for user functionality. The selected test applications in the healthcare domain target a diverse set of use case scenarios.

#### 4.5.2 Summary of information

The most relevant outcomes from the survey provided by this UC are:

- They are looking at XIFI services and facilities but their strong requirement on the healthcare data request the usage of dedicated clouds on the end-user premises (hospital for example).
- They want to use both PaaS and SaaS provisioning model but in "dedicated" environments.
- They are looking at these FI-WARE GE functionalities:

<b>Cloud Chapter</b>	<ul style="list-style-type: none"> <li>• Allocation of single VMs (image instances)</li> <li>• Job Scheduling</li> <li>• Cloud Proxy</li> </ul>
<b>Data Chapter</b>	<ul style="list-style-type: none"> <li>• Publish/Subscribe Broker</li> <li>• BigData Analysis</li> <li>• Semantic Application Support</li> <li>• Semantic Annotation</li> </ul>



<b>Apps Chapter</b>	<ul style="list-style-type: none"> <li>• Service Description Repository</li> <li>• Marketplace (part of Business Framework)</li> <li>• Light Semantic Composition</li> <li>• Service Composition</li> </ul>
<b>IoT Chapter</b>	<ul style="list-style-type: none"> <li>• (Backend) Configuration Management</li> <li>• (Backend) IoT Broker</li> <li>• (Gateway) Device Management</li> </ul>
<b>Security Chapter</b>	<ul style="list-style-type: none"> <li>• Security Monitoring</li> <li>• Identity Management</li> <li>• Privacy</li> <li>• Data Handling</li> </ul>

- In general, they plan to use all the operational services provided by XIFI (scalability, authentication/authorization, monitoring/logging etc).

#### 4.5.3 Preliminary analysis

The main challenge for FI-STAR is that the personal health data cannot be stored elsewhere than the end-user's private cloud (even doctors legitimately storing such data on their own devices while working in a hospital have the data removed from those devices as they leave the premises).

After discussing with FI-STAR about using XIFI resources, the authors understood that FI-STAR ultimate goal is to build a dedicated cloud architecture with delivery of GEs from a (local) node to the end-user. In this context the authors foresee an architecture where XIFI will provide its services on a private, not federated environment (see the scenario depicted in section 6.3).

## 5 ANALYSIS OF THE CORE BACKBONE NODES

In this section a description and an analysis is provided for the five core backbone nodes together with the constraints (if any) they are posing to XIFI. The data has been collected through a survey proposed to the infrastructure owners. The capacity data present in the following tables refers to the *current status* of the infrastructures for the Berlin, Trento and Brittany nodes. For the Waterford and Sevilla nodes the data refers to the target situation: this is due to the fact that currently these two nodes are under construction.

Anyway, taking into account the requirements collected from the XIFI Stakeholders the authors defined a list of the minimal target requirements each node should satisfy: please refer to the Section 7.1.2 for a detailed specification of them.

### 5.1 Sevilla Node Hardware

Component	Description	Comments
Servers	52 server	Brand is still unknown
Total Capacity	<ul style="list-style-type: none"> <li>CPU: 832 Cores</li> <li>RAM: 6656 GB</li> <li>HDD: 300TB</li> </ul>	
Per server capacity	<ul style="list-style-type: none"> <li>CPU : 2 PROCESSORS (8 Cores per processors, minimum 610 point of SPECint_rate_base2006)</li> <li>RAM : 128GB DDR3 Memory for 2CPU</li> <li>HDD: 16 Servers with 6TB Internal Storage, 36 Servers with 2 TB internal storage.</li> <li>2 Cabinets with 100TB of storage supporting NFS 4.2, iSCSI, FC protocols</li> <li>Network: Servers will be connected to switches with 2 redundant 10 Gigabit Interfaces.</li> </ul>	
Per core capacity	<ul style="list-style-type: none"> <li>RAM &gt; 8 GB</li> <li>HDD &gt; Scalable using cabinets.</li> </ul>	
Switch	Pending of tenders. Switches will support openflow 1.3	To be installed
Firewall	Not yet defined	To be installed

### Virtualization services

Component	Description	Comments
Hypervisor	KVM	Waiting for recommendation/specifications from FI-WARE to install it
Cloud	OpenStack and	Waiting for recommendation/specifications from FI-WARE

Manager	OpenNebula	to install it
Base OS	CentOs	Waiting for recommendation/specifications from FI-WARE to install it

### Other services

To be defined in the next months.

### Constraints

- Because the infrastructure that will be installed in Sevilla and Malaga is new, the infrastructure owner has not a priori restrictions or constraints.

### Network architecture of the Sevilla node

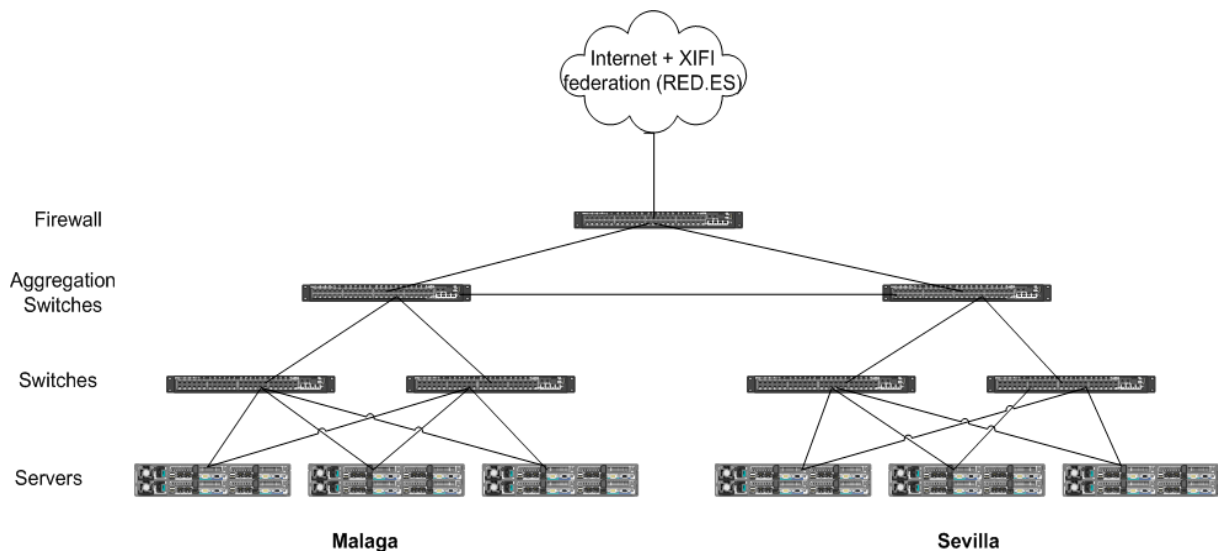


Figure 2.Malaga-Sevilla node network architecture

## 5.2 Trento Node

The following subsections describe the current status of the Trento infrastructure together with its network architecture.

### Hardware

Component	Description	Comments
Servers	3 x DELL R715	
Total Capacity	<ul style="list-style-type: none"> <li>CPU: 96 Cores</li> <li>RAM: 192 GB</li> <li>HDD: 5,4 TB</li> </ul>	
Per server capacity	<ul style="list-style-type: none"> <li>CPU : 2 x AMD Opteron 6282SE (2.6GHz, 16C, 16M L2/16M L3</li> </ul>	

	<ul style="list-style-type: none"> <li>Cache)</li> <li>RAM : 64GB DDR3 Memory for 2CPU (16x4GB Dual Rank RDIMMs) 1600MHz</li> <li>HDD: 4 X 600GB SAS 6Gb/s 10k 2,5" hot-plug</li> <li>Controller: RAID PERC H700, cache NV 512MB</li> <li>Network: 10 x Gigabit Ethernet</li> <li>Power supply: 2 x PSU 220Vac / 1.100W</li> </ul>	
Per core capacity	<ul style="list-style-type: none"> <li>RAM &gt; 2GB</li> <li>HDD &gt; 50 GB</li> </ul>	
Switch	Cisco Catalyst	to be installed.
Firewall	Fortinet Fortigate or Cisco ASA	Coupled devices for HA. To be selected and acquired (chosen among 300C-600C-ASA5545).

### Virtualization service

Component	Description	Comments
Hypervisor	KVM	Waiting for recommendation/specifications from FI-WARE to install it
Cloud Manager	OpenStack	Waiting for recommendation/specifications from FI-WARE to install it
Base OS	Debian 7 (or other if needed)	Waiting for recommendation/specifications from FI-WARE to install it

### Other services

Service	Description	Comments
Backup	unavailable	
Platform Supervisor	OpenNMS	
Platform Monitoring	OpenNMS	

### Constraints

- Access to supervision & monitoring by the XIFI federation should be investigated. Probably the target architecture should grant restricted access to XIFI hardware only.

## Network architecture of the Trento node

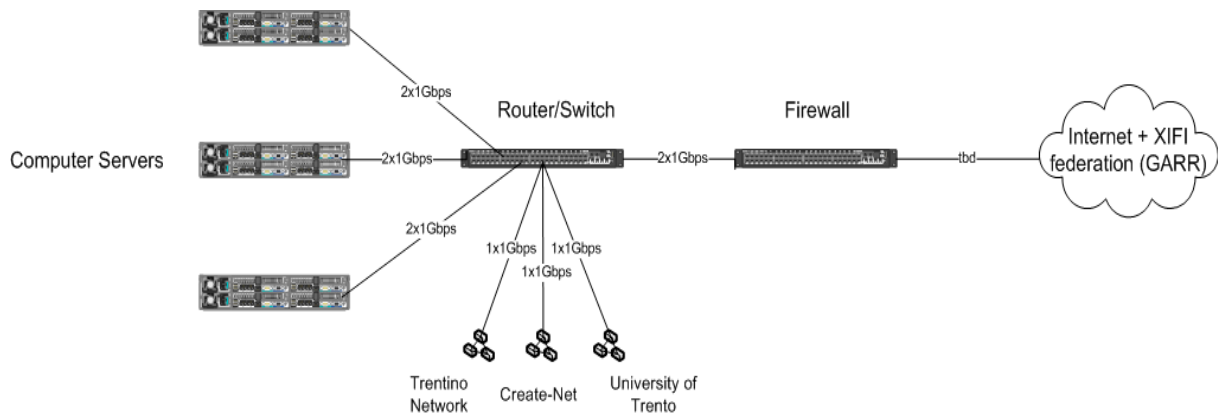


Figure 3.Trento node network architecture

## 5.3 Berlin Node

The Berlin node is a collaborative node hosted by Fraunhofer and DT. The following figure provides its architecture.

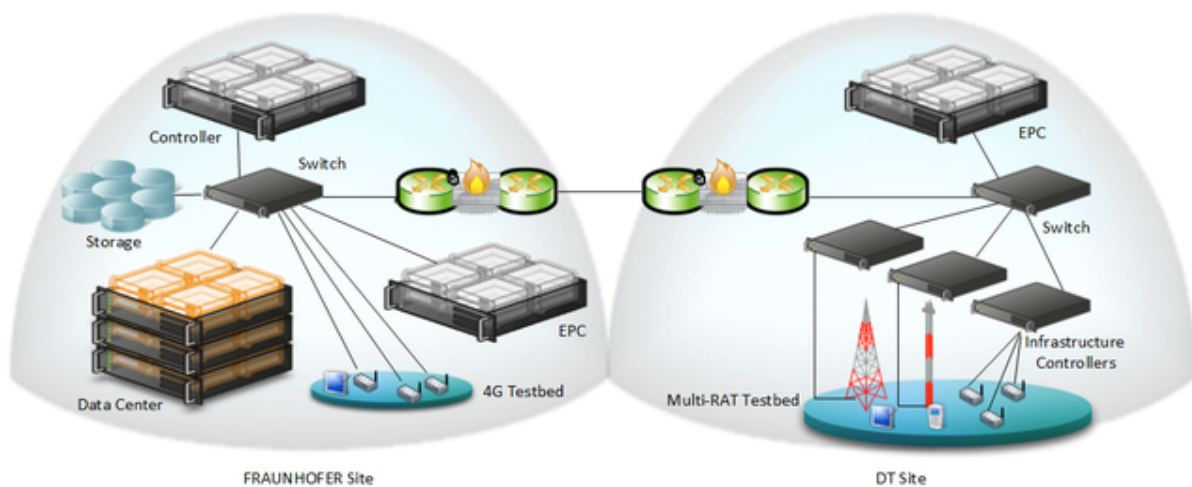


Figure 4.Architecture of the Berlin node

The following subsections describe the current status of the Berlin infrastructure together with its network architecture.

### Hardware

Component	Description	Comments
Servers	4 x DELL PE M620	
Total Capacity	<ul style="list-style-type: none"> <li>CPU: 48 Cores</li> <li>RAM: 512 GB</li> </ul>	

	<ul style="list-style-type: none"> <li>HDD: scale able shared storage (NetApp Metro Cluster)</li> </ul>	
Per server capacity	<ul style="list-style-type: none"> <li>CPU : 2 x Intel Xeon E5-2640 (2,5GHz, 6C, 15M Cache, 7,2GT/s QPI, 95W, Turbo)</li> <li>RAM : 8x 16GB RDIMM, 1.333MHz, Low Voltage, Dual Rank</li> <li>HDD: 146GB, SAS 6Gbit/s, 2,5Zoll, 15k (hosting only OS)</li> <li>Controller: H310 Controller (no RAID)</li> <li>Network: 2x Broadcom 57810-k Dual Port 10Gbit/s</li> </ul>	
Per core capacity	<ul style="list-style-type: none"> <li>RAM &gt; 10GB</li> <li>HDD &gt;scalable</li> </ul>	
Switch	Cisco Catalyst	
Firewall	Cisco ASA	

### Virtualization service

Component	Description	Comments
Hypervisor	KVM	Waiting for recommendation/specifications from FI-WARE to install it
Cloud Manager	OpenStack Grizzly	Waiting for recommendation/specifications from FI-WARE to install it
Base OS	Ubuntu 12.04.2 server 64bit	Waiting for recommendation/specifications from FI-WARE to install it

### MultiRATtestbed

Component	Description	Comments
Outdoor WiFi nodes	<ul style="list-style-type: none"> <li>9 Linux based WiFi nodes (placed outdoor).</li> <li>Each node has 4 WiFi interfaces (802.11a/b/g).</li> </ul>	
Indoor WiFi nodes	<ul style="list-style-type: none"> <li>30 indoor WiFi nodes.</li> <li>OS is configurable.</li> <li>Each node has 2 interfaces (802.11a/b/g/n).</li> </ul>	
WiMAX base station		
Femto base stations	<ul style="list-style-type: none"> <li>One 2G Femto base station from IPAccess.</li> <li>One 4G Femto base station from IPAccess.</li> </ul>	
OpenEPC	OpenEPC serves as a control layer and is running in a Proxmox/KVM based virtual environment.	
OpenIMS	OpenIMS serves as a application layer/service delivery platform and is running in a Proxmox/KVM based virtual environment.	

## Other services

Service	Description	Comments
Backup	NetApp	To be confirmed
Platform Supervisor	Nagios; Zabbix	
Platform Monitoring	Nagios; Zabbix	

## Constraints

- To use the MultiRATtestbed experimenters need to connect locally with the access networks.
- To use the 2G or 4G network of the MultiRATtestbed experimenters need to use special SIM-Cards provided by DT or Fraunhofer FOKUS.
- Experimenters should provide their own mobile device to use the MultiRATtestbed if special apps or functionalities need to be installed.

## Network architecture of the Berlin node

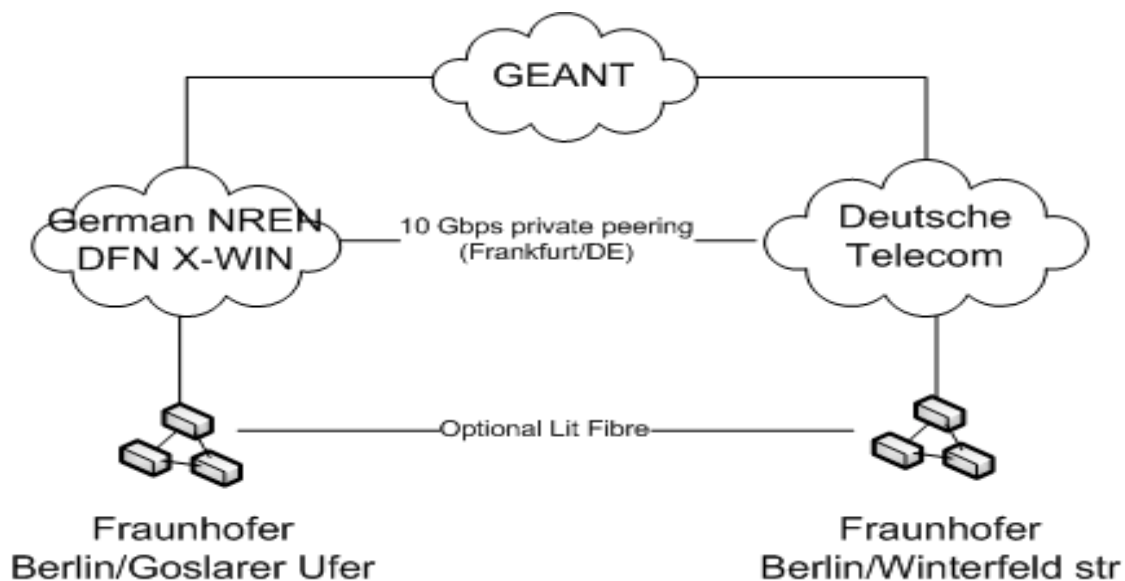


Figure 5. Berlin node network architecture

## 5.4 Brittany Node (Lannion)

The Brittany node is located in Lannion (FRANCE). The following subsections describe the current status of the Brittany infrastructure together with its network architecture.

### Hardware

Component	Description	Comments
Servers	8 x Dell power edge 6220	

Total Capacity	<ul style="list-style-type: none"> <li>CPU: 96 Cores</li> <li>RAM: 256 GB</li> <li>HDD: 36 TB</li> </ul>	
Per server capacity	<ul style="list-style-type: none"> <li>CPU : 2 x Intel Xeon E5-2640</li> <li>RAM : 32 GB 1333MHz</li> <li>HDD: 1 x 3 TB SATA 7200 rpm</li> <li>Network: 2 x Gbit Ethernet NIC</li> </ul>	
Per core capacity	<ul style="list-style-type: none"> <li>RAM &gt; 2,5GB</li> <li>HDD &gt; 250 GB</li> </ul>	
Switch	Juniper EX 3200	Juniper should release Openflow compatible firmware before the end of the year
Router/Firewall	Juniper ISG1000	Shared for all the ImaginLab platform

### Virtualization service

Component	Description	Comments
Hypervisor	KVM	Waiting for recommendation/specifications from FI-WARE to install it
Virtualization	OpenStack	Waiting for recommendation/specifications from FI-WARE to install it
Base OS	Ubuntu Server 12.04 LTS	Waiting for recommendation/specifications from FI-WARE to install it

### Other services

Service	Description	Comments
Backup	Yes (12 TBytes)	
Platform Supervisor	Nagios	
Platform Monitoring	CACTI	
LTE access network	4 eNodeBs situated at Brest	covers: tramway, road, sea, city center
FTTH acces network	2 neighbourhoods connected (~100 homes) at Lannion	FTTB also available
DVB-T2 broadcast network	Next generation terrestrial TV available at Rennes	
IMS core service	MMTel, VoLTE and other services situated	



network	at Lannion	
---------	------------	--

## Constraints

- Access to supervision & monitoring by the XIFI federation should be investigated. Probably the target architecture should grant restricted access to XIFI hardware only.

## Network architecture of the Brittany node

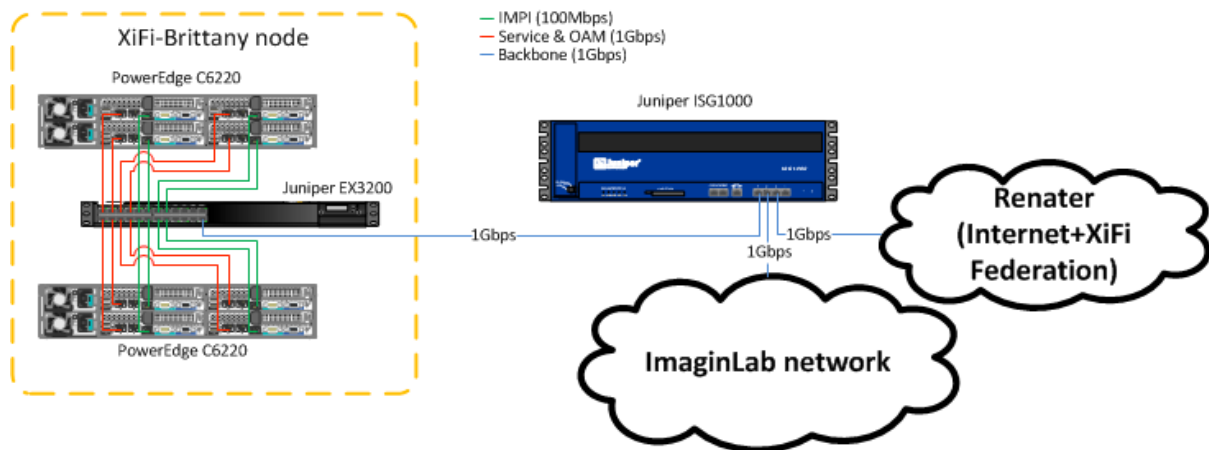


Figure 6. Brittany node network architecture

## 5.5 Waterford Node

The following subsections describe the current status of the Waterford infrastructure together with its network architecture.

### Hardware

Component	Description	Comments
Servers	12 x Dell power edge 6220	
Total Capacity	<ul style="list-style-type: none"> <li>CPU: 160 Cores</li> <li>RAM: 640 GB</li> <li>HDD: 2.040 TB</li> <li>NFS shared disk space</li> </ul>	
Per server capacity	<ul style="list-style-type: none"> <li>CPU : 2 x Intel Xeon E5-2665 (16 cores per sleigh)</li> <li>RAM : 64 GB 1333MHz</li> <li>HDD: 1 x 146 G SAS 15k disks</li> <li>Network: 2 x Gbit Ethernet NIC</li> </ul>	

Per core capacity	<ul style="list-style-type: none"> <li>RAM &gt; 4GB</li> <li>HDD &gt; 12GB</li> </ul>	
Switch	Pronto 3290	Openflow 1.2 enable via OpenVSwitch( 48 1 Gig with 4 * 10 Gig uplinks )
Firewall	Dell SonicWALL	Dell SonicWALL NSA 3500

### Virtualization service

Component	Description	Comments
Hypervisor	KVM	Waiting for recommendation/specifications from FI-WARE to install it
Virtualization	OpenStack	Waiting for recommendation/specifications from FI-WARE to install it
PXE boot	Installation of compute nodes	Automatic unattended install of latest Debian and Ubuntu KVM ( compute nodes )
Compute node Base OS	Ubuntu Server 13.04	

### Other services

Service	Description	Comments
Platform Supervisor	Nagios	event driven monitoring compute nodes and IPMI services
Platform Monitoring	Ganglia	Performance graph logging

### Constraints

- Access to supervision & monitoring by the XIFI federation should be investigated. Probably the target architecture should grant restricted access to XIFI hardware only.

## Network architecture of the Waterford node

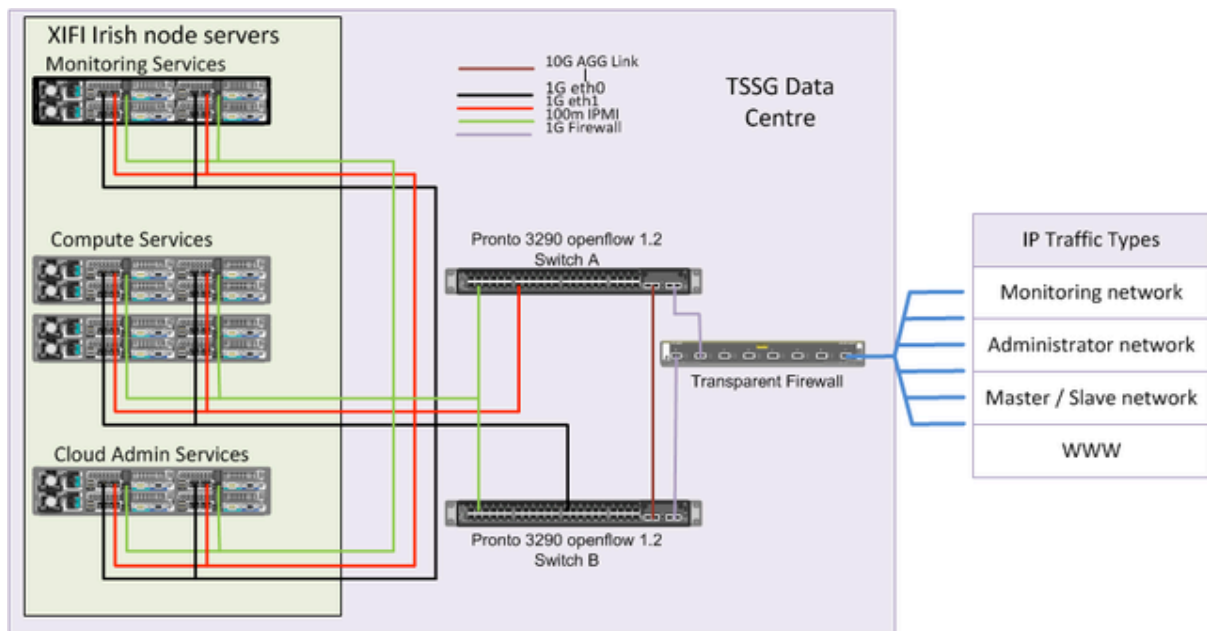


Figure 7. Waterford node network architecture

## 5.6 Summary of XIFI Nodes Features

The following table summarizes the main features of the five nodes related to services/features offered by the XIFI federation. As it appears from the table, all the nodes provide all the basic services needed by XIFI in order to build at least a federation of infrastructures fulfilling the minimal set of requirements XIFI aim to satisfy: providing a community cloud for UC projects.

Feature	Comment	Waterford	Sevilla	Trento	Berlin	Brittany
Deployment on dedicated UC machine	XIFI Site allows each UC to deploy required GES on Virtual Machines	Y	Y	Y	Y	Y
Secure access to Virtual Machines	XIFI Site allows each UC to securely access dedicated Machine	Y	Y	Y	Y	Y
Access to XIFI Site		Y	Y	Y	Y	Y

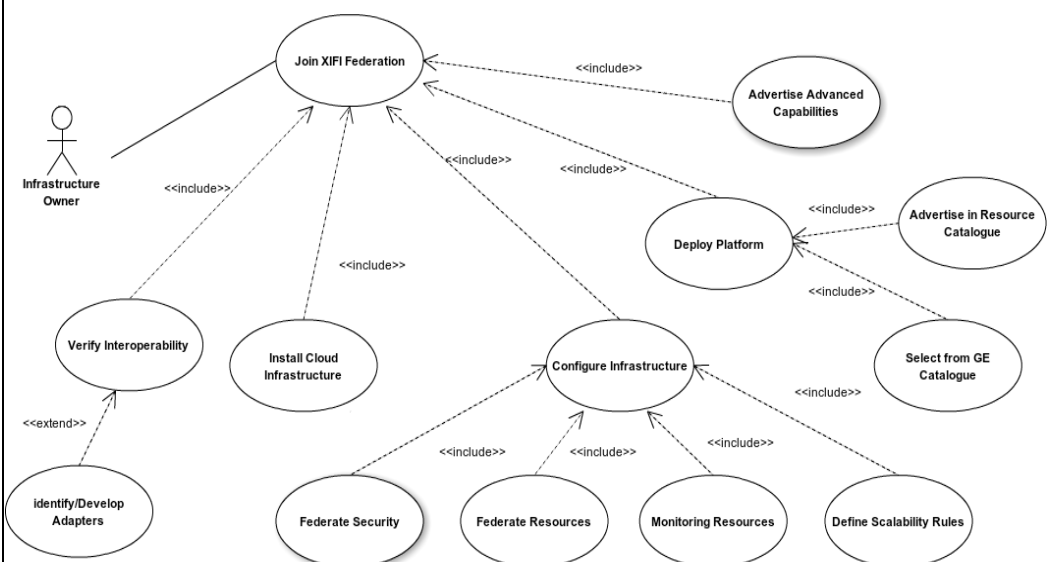
logs	allows each UC to access log files					
Public Ips	XIFI Site allows each UC to obtain a public IP address	IPv6. Limited number on IPv4	IPv6. Limited number on IPv4	IPv6. Limited number on IPv4	IPv6. Limited number on IPv4	IPv6. Limited number on IPv4
Platform Monitoring	XIFI Site provides each UC with option to monitor VM	Y	Y	Y	Y	Y
Constraints posed to XIFI	Which constraints are posed to XIFI	Restricted access to monitoring data (XIFI hw only)	none	Restricted access to monitoring data (XIFI hw only)	Access and usage of the MultIRATtestbed is restricted and constrained	Restricted access to monitoring data (XIFI hw only)

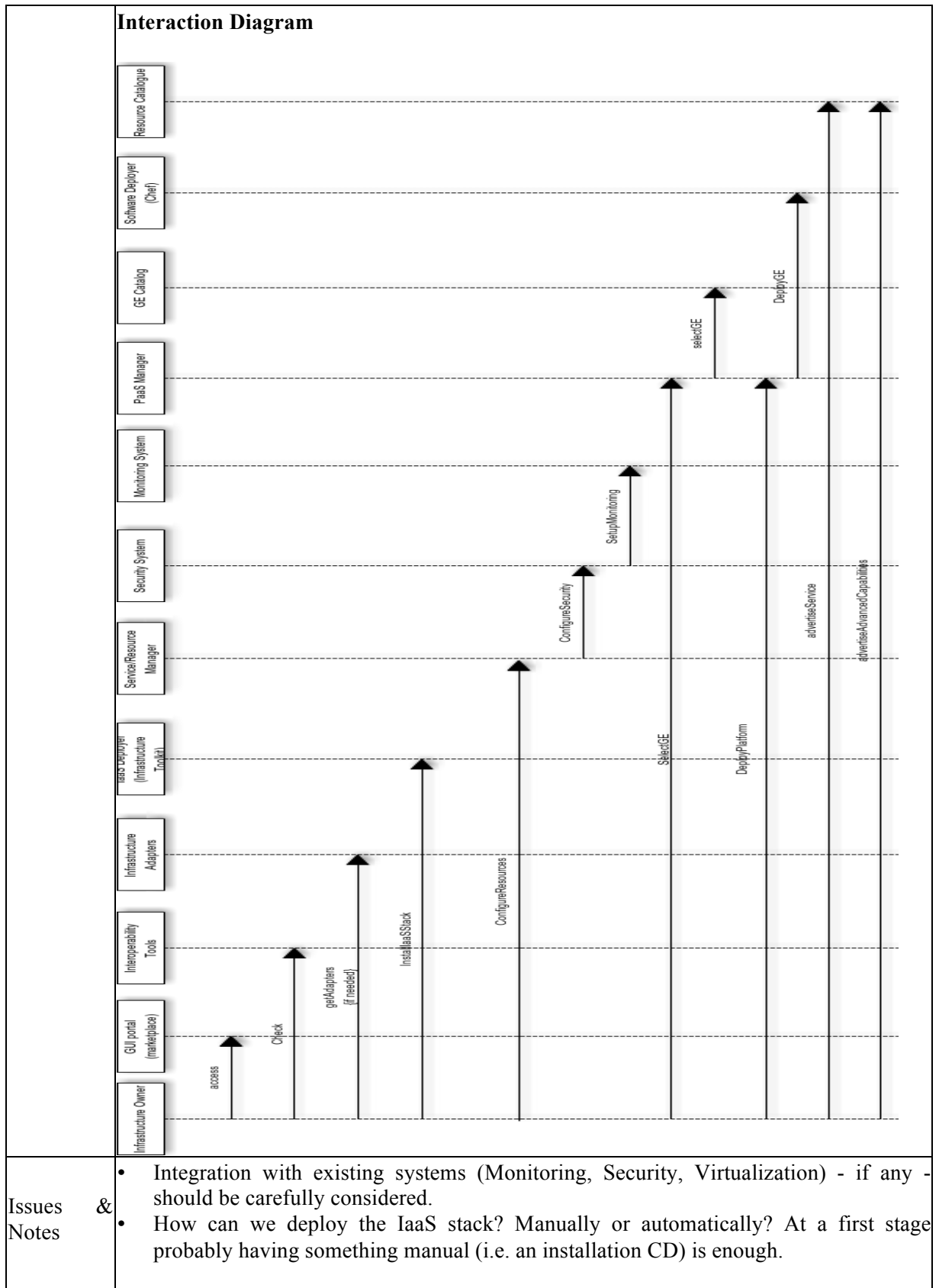
## 6 PRELIMINARY XIFI USAGE SCENARIOS AND REQUIREMENTS

From the information gathered through the surveys with the UC projects and the infrastructure owners and considering the possible XIFI stakeholder, some usage scenarios have been developed so to understand the main interactions taking place in XIFI. The following scenarios are by no means complete (detailed scenarios will be provided as result of the activities of the other XIFI technical WPs where the following scenarios will be deeper investigated) but provide an overview on the main behavioural patterns involving the different stakeholders and help to define a first draft of the architecture (see next section). The scenarios are described using a tabular format where also a use case diagram and a sequence diagram are provided.

### 6.1 An infrastructure owner wants to join the XIFI Federation

Section	Description
Use Case id	UC-1
Title & Description	Joining the federation: an infrastructure owner wants to join the XIFI Federation.
Actors	Infrastructure Owner
Use Case Objective	An owner of an infrastructure not yet part of the XIFI federation wants his/her infrastructure to join the federation
Pre-Conditions	Infrastructure owner agrees on XIFI Federation terms and conditions
Process Dialogue	<ol style="list-style-type: none"> <li>1. The infrastructure owner connects to the XIFI portal.</li> <li>2. The infrastructure owner verifies the compatibility/interoperability of his/her infrastructure: the infrastructure owner uses the relevant tools provided by XIFI in order to verify the compatibility of his/her infrastructure with the XIFI federation. <ul style="list-style-type: none"> <li>○ Identify/develop Adapters: in case it is needed in order to reach compatibility/interoperability, some adapters are selected by the XIFI catalogue and/or developed.</li> </ul> </li> <li>3. Install Cloud Infrastructure: the XIFI cloud stack software (FI-WARE IaaS) is installed on top of the “bare metal” using the services provided by XIFI.</li> <li>4. Configure Infrastructure: the new infrastructure is configured inside the federation with respect to security (identity federation), cloud resources and monitoring aspects. <ul style="list-style-type: none"> <li>○ Federate Security: a set of security services are set up (authentication, authorization, data protection etc). In particular the infrastructure secure access system (if any) is joined with the Identity Federation provided by XIFI.</li> <li>○ Federate Resources: add the infrastructure resources to the XIFI IaaS management system (FI-WARE DCRM and SM GEs) so that they can be managed as resources of the federation.</li> <li>○ Monitoring Resources: the infrastructure monitoring system (if any) is integrated with the XIFI monitoring system in order to measure performances, assure an effective use of the resources and guarantee SLAs.</li> <li>○ Define Scalability Rules: some scalability/elasticity rules are defined.</li> </ul> </li> <li>5. Deploy the new platform: the infrastructure owner selects some GEs and provides them to the developers on top of his infrastructure following a SaaS provisioning model.</li> </ol>

	<ul style="list-style-type: none"> <li>○ Select from Catalogue - the relevant GEs are selected from the XIFI/FI-WARE catalogue</li> <li>○ Advertise the new service: the new platform/service deployed is advertised in the XIFI resource catalogue</li> </ul> <p>6. The infrastructure owner advertises the advanced capabilities (e.g. sensor networks) of his/her infrastructure registering them on the XIFI resource catalogue.</p>
Variations	In some cases an adaptation layer (Adapters) may be needed to make this infrastructure "interoperable" and "compatible" with the XIFI federation.
Post-Conditions	The new infrastructure has joined the federation and is ready to provide services to the developers
Diagrams	<p><b>Use Case Diagram</b></p>  <pre> graph TD     IO[Infrastructure Owner] --&gt; JXF((Join XIFI Federation))     IDA((Identify/Develop Adapters)) -.-&gt; &lt;&lt;extend&gt;&gt;  VI((Verify Interoperability))     VI -.-&gt; JXF     ICI((Install Cloud Infrastructure)) -.-&gt; JXF     JXF -.-&gt; &lt;&lt;include&gt;&gt;  AAC((Advertise Advanced Capabilities))     JXF -.-&gt; &lt;&lt;include&gt;&gt;  DP((Deploy Platform))     JXF -.-&gt; &lt;&lt;include&gt;&gt;  CI((Configure Infrastructure))     AAC -.-&gt; &lt;&lt;include&gt;&gt;  DP     DP -.-&gt; &lt;&lt;include&gt;&gt;  ARC((Advertise in Resource Catalogue))     DP -.-&gt; &lt;&lt;include&gt;&gt;  SGC((Select from GE Catalogue))     CI -.-&gt; &lt;&lt;include&gt;&gt;  FS((Federate Security))     CI -.-&gt; &lt;&lt;include&gt;&gt;  FR((Federate Resources))     CI -.-&gt; &lt;&lt;include&gt;&gt;  MR((Monitoring Resources))     CI -.-&gt; &lt;&lt;include&gt;&gt;  DSR((Define Scalability Rules))     </pre> <p>The diagram illustrates the process of joining the XIFI Federation. The main use case is 'Join XIFI Federation', which is initiated by the 'Infrastructure Owner'. This process includes several sub-use cases: 'Verify Interoperability' (which is extended by 'Identify/Develop Adapters'), 'Install Cloud Infrastructure', 'Advertise Advanced Capabilities', 'Deploy Platform', and 'Configure Infrastructure'. The 'Deploy Platform' use case further includes 'Advertise in Resource Catalogue' and 'Select from GE Catalogue'. The 'Configure Infrastructure' use case includes 'Federate Security', 'Federate Resources', 'Monitoring Resources', and 'Define Scalability Rules'.</p>

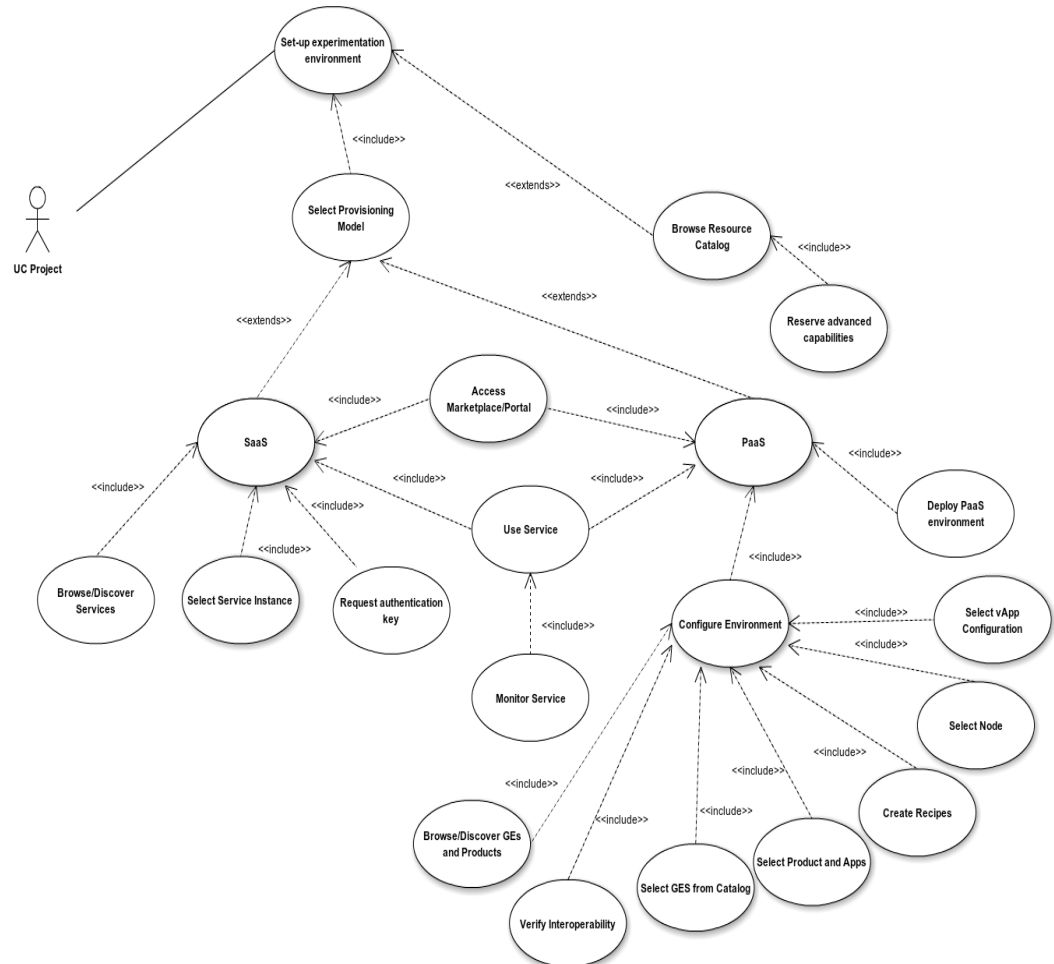


## 6.2 A UC project wants to setup and use an experimentation environment

Section	Description
Use Case id	UC-2
Title & Description	A UC project wants to use the services offered by the XIFI platform in order to develop and test innovative applications (Setup and usage of an experimentation environment).
Actors	UC project
Use Case Objective	A UC project sets up a development/test environment for experimenting innovative applications
Pre-Conditions	UC project agrees on XIFI Federation terms and conditions
Process Dialogue	<ol style="list-style-type: none"> <li>The UC project accesses to the XIFI marketplace/portal.</li> <li>The UC project selects the provisioning model it wants to use: either SaaS or PaaS</li> <li>In case of SaaS: <ul style="list-style-type: none"> <li>The UC project browses the marketplace for existing service(s). Here tools like a resource catalogue, a recommender and some monitoring/SLA/QoS tools come into play. For example the UC project can be guided in its choices by a recommender or can base its selection on the QoS levels.</li> <li>The UC project selects the instance/endpoint where the service is provided</li> <li>The UC project gets the authorization key through an access control system and uses the service</li> <li>the service performances are monitored by the monitoring system</li> </ul> </li> <li>In case of PaaS: <ul style="list-style-type: none"> <li>The UC project has to configure and create the development/testing environment: <ul style="list-style-type: none"> <li>The UC project browses the GE and product catalogues for finding the GEs and products it wants. Here tools like a PaaS manager and interoperability check tools come into play:</li> <li>verify interoperability of UC software design with the rest of the environment (GEs, APIs etc)</li> <li>selects the needed GEs (the GEs are contained in the GE catalogue),</li> <li>selects third party COTS and applications,</li> <li>prepares the recipes for sw deployment (like Chef recipes),</li> <li>selects the node where the deployment should be made</li> <li>selects the number and flavour of the virtual machines</li> </ul> </li> <li>the software is deployed and used</li> <li>the service performances are monitored by the monitoring system and the QoS and the SLA verified</li> </ul> </li> <li>In case of specific needs, the UC project can browse the XIFI resource catalogue in order to find advanced capabilities advertised by the infrastructures (e.g. sensor networks, mobile networks etc). Then it can reserve those capabilities for his experimentation.</li> </ol>
Variations	The UC project can opt for a SaaS provisioning model or a PaaS one.
Post-Conditions	The development/test environment is up & running



## Use Case Diagram

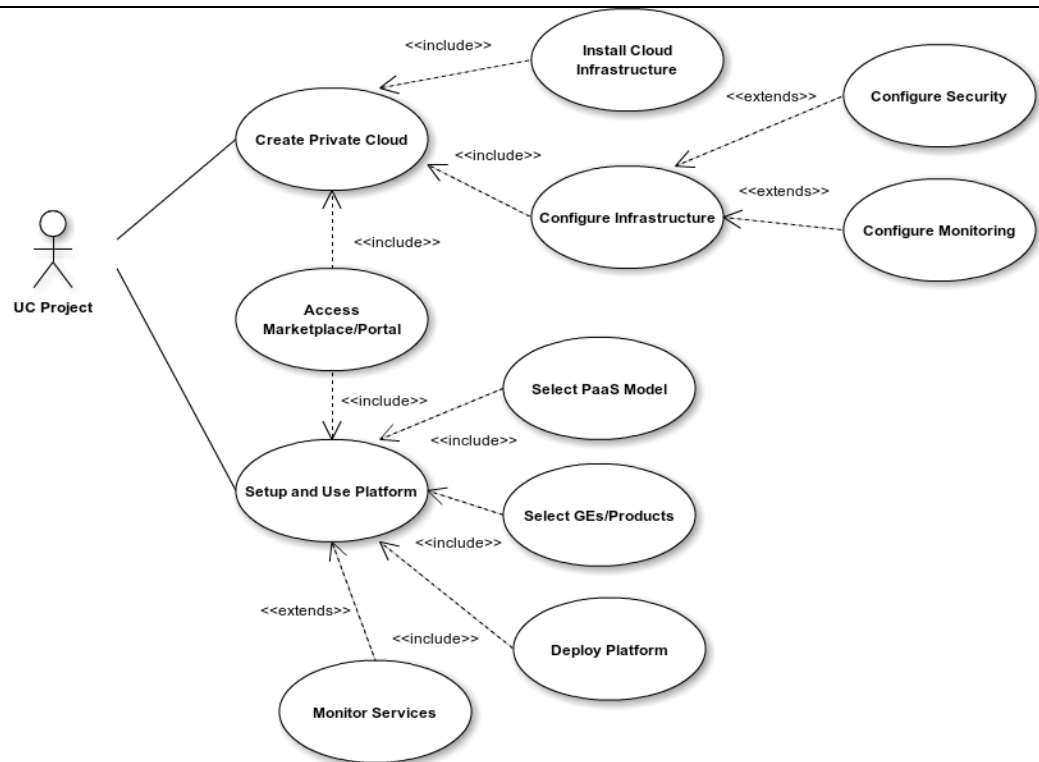


Diagrams

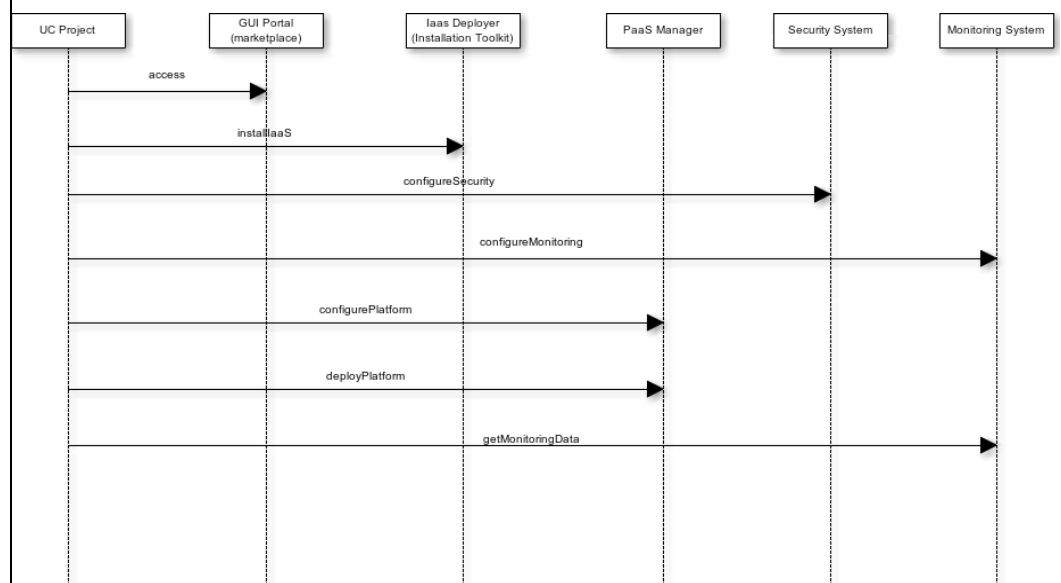


### 6.3 In order to set-up a cloud infrastructure (non federated with XIFI), XIFI services are used

Section	Description
Use Case id	UC-3
Title & Description	<p>The developer creates and uses his private cloud using the XIFI federation services.</p> <p>This scenario show how a private cloud can be set up using the XIFI services and then used as a cloud infrastructure completely dedicated to an UC project. Nevertheless some XIFI federated services like monitoring and/or SLA Management can be used to support the cloud management.</p>
Actors	UC project
Use Case Objective	The UC project wants to create a private cloud dedicated to its experiments.
Pre-Conditions	<p>The use case project wants to use its own infrastructure to be provided as a private node.</p> <p>(UC project agrees on XIFI Federation terms and conditions).</p>
Process Dialogue	<p>Two main step can be differentiated:</p> <ol style="list-style-type: none"> <li>The UC project creates a "private cloud": <ul style="list-style-type: none"> <li>The UC project connects to the XIFI portal.</li> <li>The UC project installs on its private resources the FI-WARE cloud stack software. It uses the XIFI installation toolkit to install the cloud stack software and all the necessary components and adapters (see UC-1)</li> <li>(if requested by the UC project) The private infrastructure is configured so to use XIFI services like security (identity federation) and monitoring.</li> <li>The administration and usage of the “private cloud” is totally managed by the UC project.</li> </ul> </li> <li>After the FI-WARE cloud stack software has been configured, a PaaS can be created (see scenario UC-2). <ul style="list-style-type: none"> <li>The UC project connects to the XIFI portal.</li> <li>The UC project selects the PaaS provisioning model.</li> <li>The UC project can configure its private cloud, selecting the VM configuration, the GEs, the third party COTS and applications.</li> <li>The XIFI PaaS manager builds the platform with all the elements requested.</li> <li>XIFI tools for monitoring the performance of this private cloud can be set up (if requested by the UC project).</li> </ul> </li> </ol>
Variations	Of course the UC project can also install its private infrastructure using its own tools avoiding any relation and usage of XIFI tools/services. But in this case the installed components and in general the private infrastructure cannot be managed through XIFI services. Moreover in the future a possible integration with XIFI will be very difficult.
Post-Conditions	The private cloud has been created.
Diagrams	<b>Use Case Diagram</b>



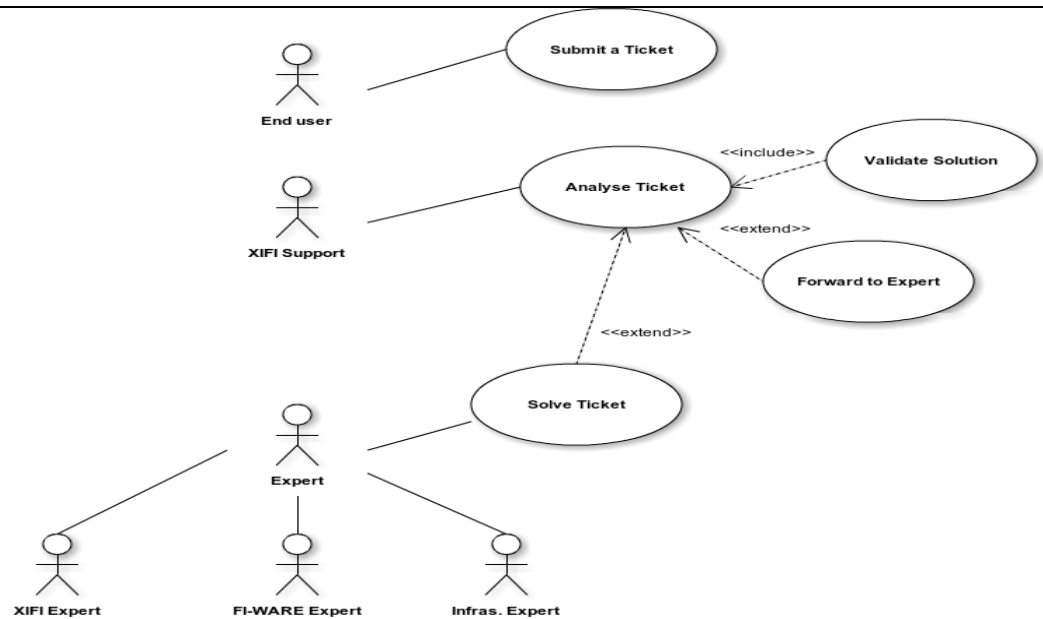
### Interaction Diagram



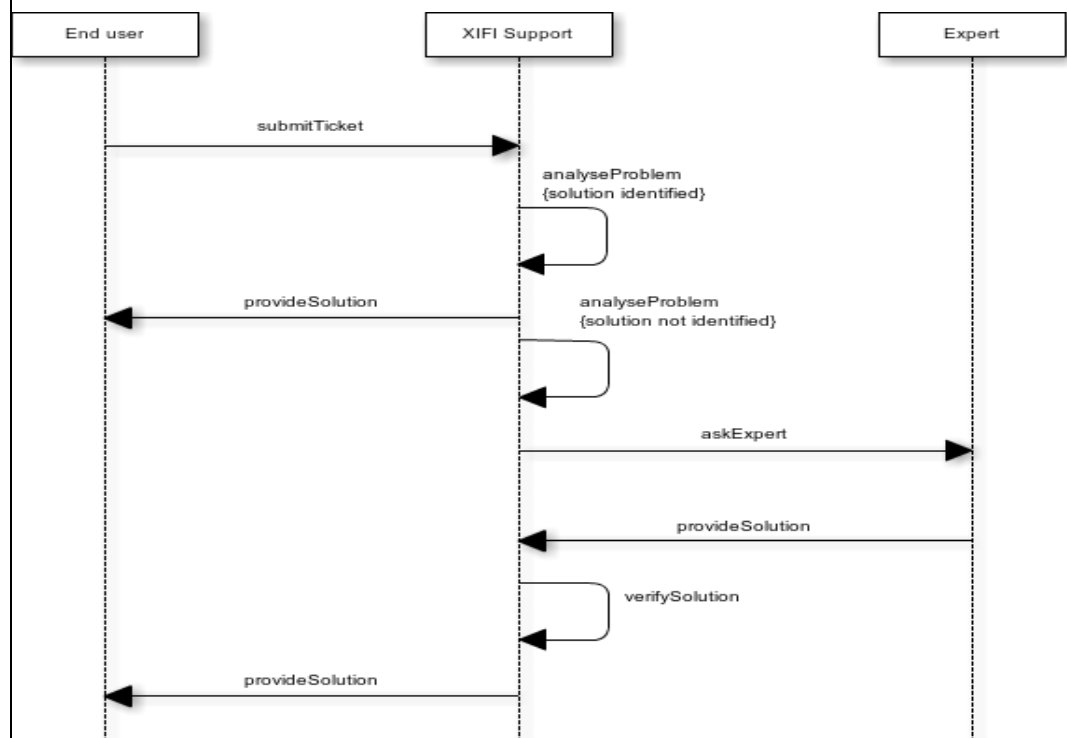
Issues & Notes

#### 6.4 An end-user of the Federation requests support and help

Section	Description
Use Case id	UC-4
Title & Description	User Support: an end-user of the XIFI Federation needs help.
Actors	End user of the XIFI Federation (mainly a UC project developer or a Future Internet experimenter)
Use Case Objective	Solve issues related to XIFI services and resources, address support request, track problems until their resolution
Pre-Conditions	The end user has an account on XIFI and has access to the XIFI Helpdesk tool through the federation portal
Process Dialogue	<ol style="list-style-type: none"> <li>1. The end user identifies an issue or a request he wants to address to XIFI.</li> <li>2. The end user connects to the Helpdesk through the XIFI portal.</li> <li>3. The end user opens a ticket describing the problem and addresses it to XIFI support (first level of support).</li> <li>4. XIFI contact the user and replicate the issue (so that it's clear don't depend from the user's device)</li> <li>5. XIFI support analyzes, diagnoses and isolates the problem. At this point it can either: <ul style="list-style-type: none"> <li>o Identify a solution and propose it to the user</li> <li>o Report the issue to an expert (second level of support): <ul style="list-style-type: none"> <li>▪ If the issue is related with XIFI services, it is forwarded to a XIFI expert</li> <li>▪ If the issue is related with FI-WARE GEs, it is forwarded to a FI-WARE expert</li> <li>▪ If the issue is related with an infrastructure resource, it is forwarded to the infrastructure expert.</li> <li>▪ Assuming the issue is reported an expert, he will perform an analysis and provide a solution.</li> </ul> </li> </ul> </li> <li>6. XIFI support should apply the solution given and demonstrate that the problem doesn't occur anymore. If not, he returns to the expert.</li> <li>7. If the solution is viable, the XIFI support provides the solution to the user.</li> <li>8. If the problem is solved, XIFI support document the solution in the system for future reference and closes the ticket. Otherwise other iterations occur.</li> </ol>
Variations	
Post-Conditions	A solution should be always provided to the end user. This solution must preserve the SLA contracted with the end user (see 7.1.14).
Diagrams	<b>Use Case Diagram</b>



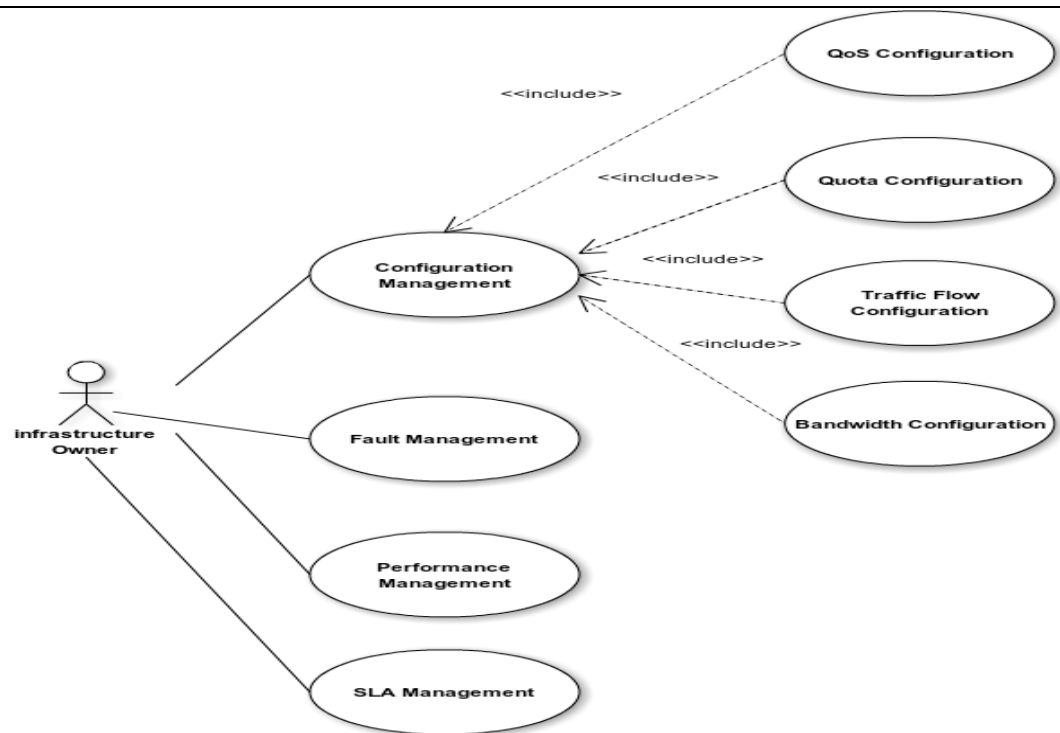
### Interaction Diagram



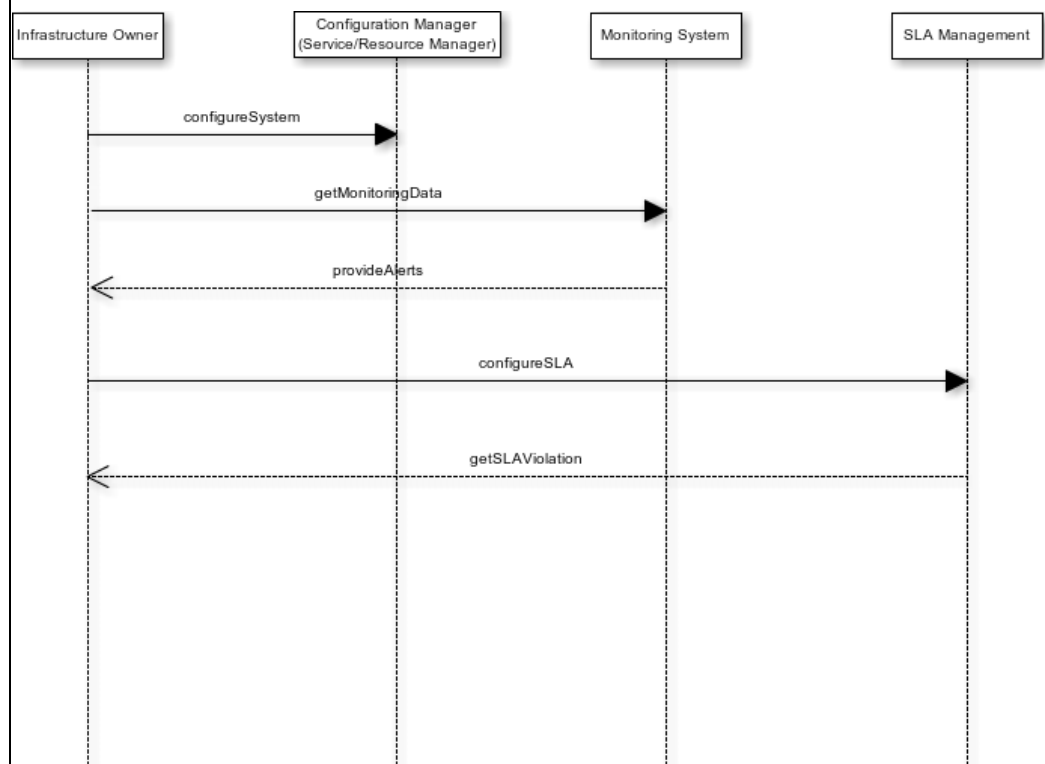
Issues & Notes

## 6.5 Management of an Infrastructure (Network and Data Center)

Section	Description
Use Case id	UC-5
Title & Description	Network and Data Center operations
Actors	Infrastructure Owner
Use Case Objective	Keep both network and data center under a reliable functioning condition, according to end users specific needs and actual performance
Pre-Conditions	Infrastructure has joined the XIFI Federation (see UC-1)
Process Dialogue	<ol style="list-style-type: none"> <li>1. The infrastructure owner configures the infrastructure so to define levels and ranges of QoS, bandwidth, quotas (i.e. disk, cores, bandwidth), traffic flow, SLA etc (Configuration Management)</li> <li>2. The infrastructure owner check possible faults in the network and data center (Fault Management): infrastructure owner needs to keep a constant monitoring on both network and data center in order to control possible glitches or disruption of the services</li> <li>3. The infrastructure owner check possible violation of defined SLAs (SLA Management): SLAs set up with end users should be monitored in order to verify their violations.</li> <li>4. The infrastructure owner check network and data center performances in order to understand and foresee possible service disruptions (Performance Management).</li> </ol>
Variations	NA
Post-Conditions	The infrastructure is set up and configured in order to sustain the user demands and possible unexpected disruption of the provided services
Diagrams	<b>Use Case Diagram</b>



### Interaction Diagram



Issues &  
Notes



## 7 DRAFT OF THE ARCHITECTURE OF XIFI FEDERATED PLATFORM

In the previous sections we collected all the material needed to provide a first draft of the XIFI architecture. The following subsections are devoted to the description of the XIFI architecture from both a technical and business point of view.

### 7.1 Technical Architecture

In the section a first draft of the technical architecture is provided. In particular we give a description of the physical (deployment) architecture, of the logical architecture and of the minimal requirements a node of the federation should satisfy in order to join the XIFI federation. The architecture presented is the target architecture, and different steps may be needed to achieve it. So it may not reflect the first version of available XIFI platform functionalities pending on availability of resources and release of up-to-date GEs supporting the new requirements posed by the architecture.

#### 7.1.1 Overview

As stated in the XIFI Dow [1] and in the previous scenarios, there are mainly three ways for provisioning services in XIFI: SaaS (Software as a Service)<sup>4</sup>, PaaS (Platform as a Service)<sup>5</sup> and IaaS (Infrastructure as a Service) provisioning models. The last one is the lowest common layer on which the other two trust.

The first one is based on the sharing of the same software platform and services among different users/experimenters (and implies that the service supports multiple tenants):

- the user identifies a GE or a third party product he wants to use
- the user selects an endpoint where the service is provided
- the user applies for a security key
- the user start playing with the service

The second one provides a platform built for and dedicated to a given user/experimenter:

- the user identifies set of GEs or third party products he wants to use
- (optional) the user select one or more nodes (data centers) where he wants to deploy the new platform
- the user deploys the new platform (composed by the GEs/products selected)
- the platform is deployed and ready for use.

The following figure presents in a graphical manner what described.

---

<sup>4</sup>“The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.” [2]

<sup>5</sup>“The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.” [2]

## Software as a Service

## Platform as a Service

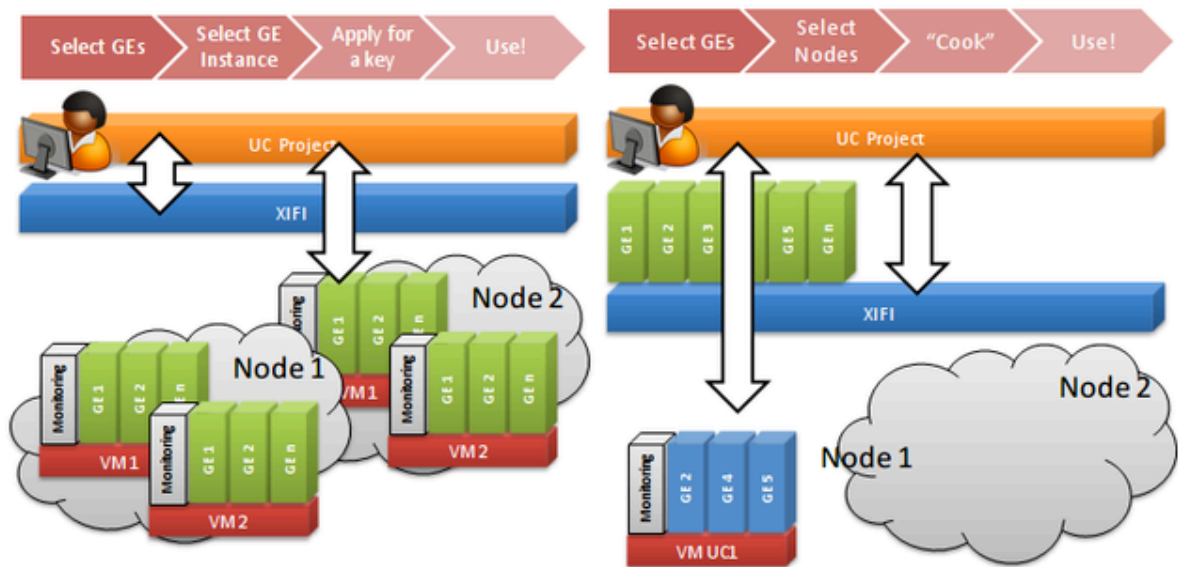


Figure 8.SaaS vs PaaS

Of course this process can be applicable only to services that can be delivered and in an "automatic" way (i.e. without any manual intervention and/or negotiation between the user and the XIFI Consortium). For special services requiring the human intervention and negotiation (as for instance access to sensor networks, LTE networks etc.), the authors foresee a direct interaction between the user and the infrastructure owner. Nevertheless, the aforementioned behaviour, where automatic interactions can be applied, covers the majority of the cases of usage of XIFI.

From the previous picture it could appear that all the nodes of the federation are equivalent. In fact this is not the case if a robust and sustainable architecture should be deployed:

1. from one side having all the XIFI federation services and repositories (like monitoring, security, portal, catalogues etc.) distributed on all the nodes can complicate a lot the management of the federation (think in particular to the synchronization problems among the different nodes);
2. but from the other side, having all the XIFI services on just one node does not assure high availability.

For this reason the authors foresee a deployment configuration as depicted in the following figure where two nodes are considered as masters and the other three as slaves: the master nodes are the ones where, in addition to the features deployed on the slave nodes, the centralized parts of the federation services (i.e. the components needed to manage the federation) are deployed whilst the slaves ones are the nodes where only the software needed for deploying and managing user services is installed.

Note: please consider that not all the relations among the nodes are depicted.

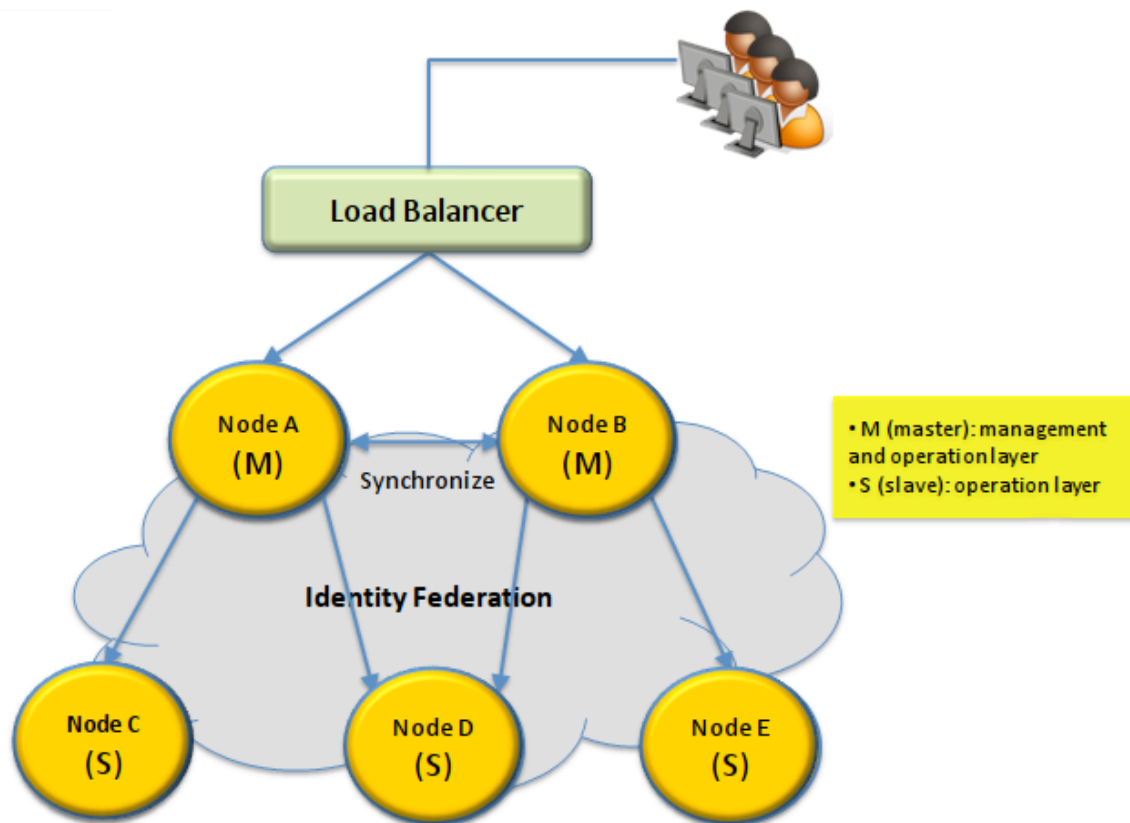


Figure 9. XIFI deployment architecture

### 7.1.2 Minimal network and capacity requirements for each node

At the moment of this writing, the authors still have to decide the detailed characteristics of each master node with respect to the ones of a slave node; moreover the properties of the network links between a master and a slave node or between two master or two slave nodes should be carefully defined. Nevertheless, checking also the information provided by the five infrastructure nodes (see previous section where the infrastructures have been described), the authors can argue a sort of minimal requirements for each node that are listed hereunder:

- Connectivity:
  - Inter node connectivity will be done via classical routing. P2P and other solutions will be evaluated later on.
  - Backbone will be implemented in IPv6
  - Service to end users will be provided in dual stack IPv4 / IPv6
  - Bandwidth between two master nodes should be at least of 1 Gbps
  - It would be nice if also the bandwidth among the other nodes would be of 1 Gbps
  - Internet connectivity (at least 100 Mbps)
- Hardware (for each node):
  - 100 CPU cores
  - Core types: Intel VT-x or AMD AMD-v
  - RAM 2 GB x Core
  - HD 20 GB x Core

- SEC Firewall

Moreover the authors foresee the need to have quite a lot of flexibility on these values in order to accommodate UC needs. For this reason each node should be equipped in order to scale doubling at least the hardware capacity stated above

### 7.1.3 FI-WARE Cloud Hosting Main Constraints

Since the XIFI Architecture is based on the FI-WARE Cloud Hosting architecture, it is important to understand the constraints posed by the installation of these software components in particular in terms of hardware and software requirements. At this stage of the project the authors do not have enough information to precisely define the constraints posed by each GE (and probably this isn't so important for some GEs where the requested resources strongly depend from many factors like for example the number and type of users), but it is very important to define the main constraints for the installation of the FI-WARE Cloud Hosting software stack. The DataCenter Resource Management (DCRM) GE [7] is the main component of the cloud stack software and the one for which FI-WARE has provided the following main requirements:

- Software requirements
  - operating system: Ubuntu 12.04
  - hypervisor: KVM
  - IaaS Manager: OpenStackGrizzly version (all basic components plus Quantum and Swift)
- Hardware requirements
  - CPU: 8 cores ( $\geq 2.4$  GHz, VT-x enabled)
  - RAM: 16GB
  - Disk Space: 1TB

Each infrastructure joining the XIFI federation should be guaranteed at least the aforementioned list of requirements. As already said, these are the first set of requirements posed by FI-WARE IaaS Management. In the future they can change and/or other can be added.

### 7.1.4 XIFI Logical Architecture

In the following the main components of XIFI have been identified and described taking into account the scenarios developed in the previous section. This is the list of the architectural components identified:

- Marketplace
- Resources Catalogue (Yellow Pages)
- Recommendation Tool
- Interoperability Tools
- Infrastructure Toolbox
- Federation Service and Resource Manager
- PaaS Manager
- Federation Security and Security Dashboard
- Federation Monitoring
- SLA Management
- HelpDesk

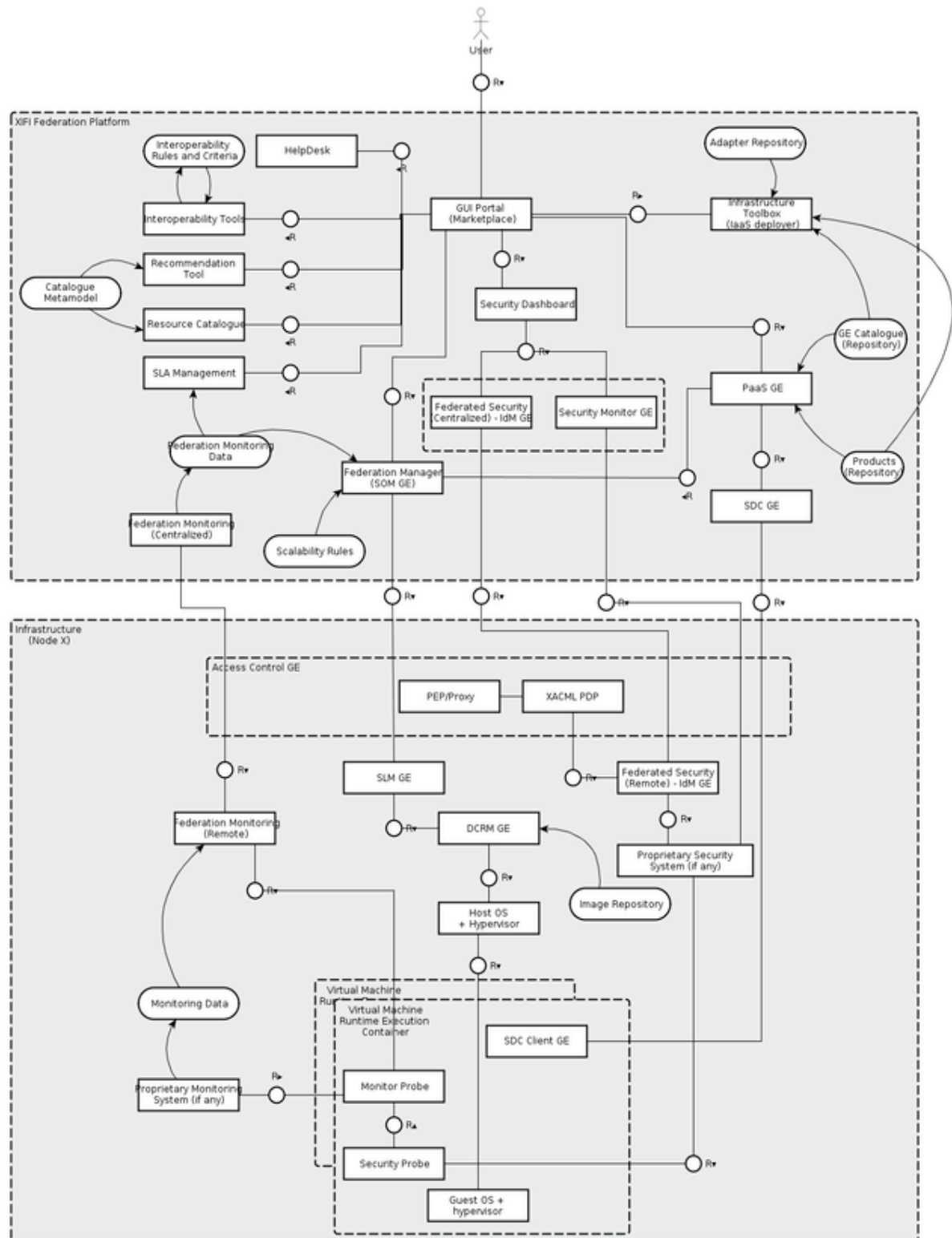


Figure 10.XIFI general FMC compositional structure diagram

The above figure shows the FMC compositional structure diagram highlighting the relations among the components. The lower square represents a generic node of the XIFI federation whereas the upper

square contains the “federation services”, i.e. the services offered to support the management and provisioning of resources in a unified fashion. Such services are located only in the master nodes. To support high availability of XIFI platform, a number of services are provided by each node of the federation. This avoids any disruption in case the master nodes experienced some outage. This is the case for example of the security system where the IdM and Access Control functionalities are distributed on all the nodes in order to allow the end users to access the XIFI services hosted on a particular node even though the central authentication and authorization system is down. Similar considerations can be applied to the monitoring system.

For the meaning of the acronyms related to the FI-WARE GEs, please see the corresponding FI-WARE documentation. It should be mentioned here that this architecture diagram has been presented and then validated inside the XIFI/FI-WARE architectural working group (see section 3.4).

For each component identified, a description is given in the following tables.

### 7.1.5 Marketplace

Section	Description
Component name	Marketplace
Component Description and Functionalities	<p>It is the Single Entry Point (Portal) where the XIFI users (UC/developers but also infrastructure owners) gain access to the XIFI federated resources/services. This portal integrates a collection of distributed and federated services such as:</p> <ul style="list-style-type: none"> <li>• Resource Catalogue/Yellow Pages: where the infrastructure capabilities and GEs endpoints deployed (in a SaaS model) are advertised</li> <li>• Security Dashboard/Federation Security: where all the tools and functionalities for managing the security and privacy of the resources in the federation can be accessed</li> <li>• Monitoring and SLA Management: where the monitoring data and SLA monitoring/management functionalities are provided</li> <li>• Interoperability Tools: where the interoperability and compatibility between interfaces of two different components can be verified</li> <li>• Infrastructure Toolbox (IaaS Deployment): where the tools for deploying the IaaS stack can be accessed</li> <li>• PaaS Manager that provides functionalities for browsing GEs/SEs and product catalogues and deploying them</li> <li>• Federation Service and Resource Manager: where the IaaS stack in terms of virtual appliances, virtual data centers and projects (intended as the container of a set of vApp belonging to a unique administrative entity) can be managed.</li> <li>• HelpDesk tool that provide functionalities related to the user support (issuing a ticket, reporting a problem, contacting support etc).</li> </ul>
Interfaces Exposed	<ol style="list-style-type: none"> <li>1. GUI towards the user</li> <li>2. Mashup Portal</li> </ol>
Interfaces Requested	<ol style="list-style-type: none"> <li>1. SSO System (IdM GE) - SAML/OAuth2 or other</li> </ol>
Behaviour	<p>It is a portal, so the behaviour is driven by the users:</p> <ol style="list-style-type: none"> <li>1. user login</li> </ol>

	<ol style="list-style-type: none"> <li>2. user select a tool/functionality</li> <li>3. user plays with a tool</li> <li>4. user logout</li> </ol>
Instances and Deployment	Deployed in high availability mode: two redundant instances located on two different <i>master</i> nodes of the federation.
Issues & Notes	The FIWARE Application Mashup - Wirecloud GE can be used to implement the XIFI marketplace

### 7.1.6 Resource Catalogue

Section	Description
Component name	Resource Catalogue
Component Description and Functionalities	<p>It represents the catalogue where available information on infrastructures can be found:</p> <ul style="list-style-type: none"> <li>the endpoints of the GEs instances deployed (SaaS model)</li> <li>the data center capabilities for hosting a software platform</li> <li>other capabilities as the presence of Sensor Network, Mobile Network and in general other features different from the bare data center.</li> </ul> <p>For each exposed service/resource, the user can also check the monitoring and performance data when it is available.</p> <p>The component is mainly used by a developer that wants to find and access the XIFI federated resources/services and the infrastructure owner that want to advertise the services provided by his infrastructure through this component. The user can browse/search the catalogue of the services/resources offered and find what he/she needs:</p> <ul style="list-style-type: none"> <li>for the SaaS services the user get the endpoint of the services and the keys to use it</li> <li>for other <i>non-conventional</i> services the user can gather their properties and characteristics and obtain the contact information of the infrastructure owner in order to ask him or negotiate with him the offer details.</li> </ul> <p>In order to provide its functionalities (in particular search and discovery), this component trust on the <i>Catalogue Metamodel store</i>, that is a common model describing all the element of the XIFI catalogue in an abstract manner (ie resources, services, GEs, products etc),</p>
Interfaces Exposed	This component exposes a GUI that will be integrated into the Marketplace portal. So it should be compliant with the mashup integration in the Marketplace portal. Nevertheless it exposes also RESTful APIs to access its functionalities.
Interfaces Requested	<ul style="list-style-type: none"> <li>with the SSO system (OAuth) in order to obtain the keys to use the services endpoints</li> <li>with the Federation Monitoring and the SLA Management components in order to gather the relevant monitoring and SLA data for each services advertised. This is a RESTful API.</li> <li>with the <i>Catalogue Metamodel store</i> in order to get the model of the</li> </ul>



	resources/services/GEs advertised.
Behaviour	<ol style="list-style-type: none"> <li>1. The user can browse the services offered or search for a specific service using some search criteria.</li> <li>2. The user can select a specific service/resource and view the information related with it (parameters, location, monitoring data etc)</li> <li>3. The user can get in contact with the infrastructure owner in order to obtain more information on non-conventional services</li> <li>4. The user can obtain the grants/keys to use a service and be redirected to its implementation.</li> </ol>
Instances and Deployment	As per the Marketplace component
Issues & Notes	

### 7.1.7 Recommendation Tool

Section	Description
Component name	Recommendation Tool
Component Description and Functionalities	<p>This component is an add-on to the Resource Catalogue (Yellow Pages) component and offers functionalities that can help the user to find the right resource/service he/she needs.</p> <p>The component is mainly used by a developer that wants to find and access the XIFI federated resources/services. Based on the requirements expressed and submitted by the user (in terms of capacity, security, SLA, and functionality needed), the tool selects the set of resources/services or software components that best match the user requirements and presents them to the user and or provide a comparison between two resources/services based on some criteria.</p> <p>In order to provide its functionalities, this component trust on the <i>Catalogue Metamodel store</i>, that provides a common model describing all the element of the XIFI catalogue in an abstract manner (ie resources, services, GEs, products etc).</p>
Interfaces Exposed	This component exposes a GUI that will be integrated into the Marketplace portal. Nevertheless it exposes also RESTful APIs to access its functionalities.
Interfaces Requested	<ul style="list-style-type: none"> <li>• with the <i>Catalogue Metamodel store</i> in order to get the model of the resources/services/GEs advertised.</li> </ul>
Behaviour	<ol style="list-style-type: none"> <li>1. The user provides some requirements in terms of: capacity, security, SLA, and functionality needed</li> <li>2. The tool, using some criteria defined and the <i>Catalogue Metamodel</i>, provides the user with the solutions that best fit his/her needs.</li> </ol>
Instances and Deployment	As per the Marketplace component
Issues & Notes	



### 7.1.8 Interoperability Tools

Section	Description
Component name	Interoperability Tools
Component Description and Functionalities	<p>The Interoperability Tool supports the specification and execution of <b>interoperability rules and criteria</b> against Future Internet software-based services. Such interoperability rules and criteria capture re-usable composition patterns of Generic Enabler functionality to orchestrations of Generic Enabler functionality, i.e. a specification that states how the service APIs are composed and invoked in sequence and what interoperability requirements must be adhered to. Therefore, when an interoperability test is executed the software service can be evaluated with regards to the extent that such interoperability is achieved. This tool is then utilised by different stakeholders of the XIFI Federation in order to check their interoperability claims:</p> <ul style="list-style-type: none"> <li>• <b>Future Internet Application Developers</b> (e.g. FI-PPP Use Case Trial developers): use the Interoperability Tool during the system development and testing phase to assess how their software (e.g. a set of SEs) interoperates within different interoperability rules and criteria. <i>Business Value: supporting early interoperability testing and identifying how they can leverage GE orchestrations, will significantly reduce the application development time.</i></li> <li>• <b>Developer/Owner of a new Enabler</b>: uses the Interoperability tool to test the compliance of their implementation of a service interface within the orchestrations, i.e., it verifies that a new service (enabler) can replace another, reporting any interoperability problems. <i>Business Value: Interoperability and compliance testing is an expensive and time consuming task; the tool seeks to automate a high-percentage of this process to reduce time and costs.</i></li> <li>• <b>Infrastructure Owners</b>: use the tool to select and execute the orchestration models to verify the behaviour of their node within a wider federation of infrastructures. <i>Business Value: i) support for future certification of interoperability within the federation; ii) allow infrastructures to verify and publish which of the orchestration patterns they can support, i.e. they can highlight both their generality and their novelty of services.</i></li> </ul>
Interfaces Exposed	This component provides a GUI to its users. This interface will be integrated into the XIFI Marketplace portal in order to be widely available from a common/trusted source. Further, it exposes a RESTful API to allow computational elements to leverage its functionalities.
Interfaces Requested	<ul style="list-style-type: none"> <li>• The <i>Catalogue Metamodel</i> to retrieve detailed information about particular resources and services..</li> <li>• The <i>interoperability rules and criteria store</i>, which is a XIFI repository of the interoperability orchestration specifications.</li> </ul>
Behaviour	<p>FI experimenter/developer :</p> <ol style="list-style-type: none"> <li>1. The FI experimenter hosts their new SE services with reachable endpoints.</li> </ol>

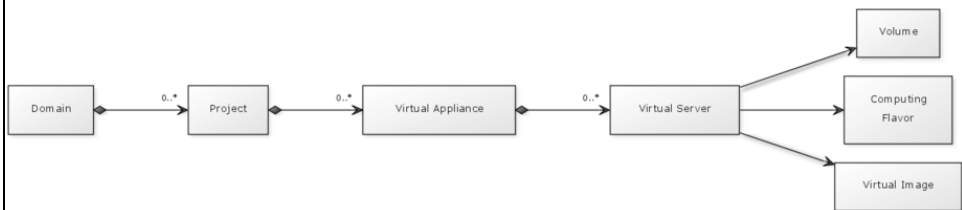
	<ol style="list-style-type: none"> <li>The user selects an interoperability orchestration pattern that they wish to evaluate their software against (or they use the tool to edit/specify a new interoperability orchestration).</li> <li>Within this pattern the user will select the elements from step one that he wishes to evaluate with respect to these elements being interoperable within the orchestration (there is no need to evaluate all the components/GEs).</li> <li>The tool, based on the evaluation criteria and on the common models for the resources, provides as output to the user: an evaluation of the interoperability of the SEs described in step 1 with the GEs.</li> </ol> <p>New GE developer:</p> <ol style="list-style-type: none"> <li>The developer hosts their new single GE service with a reachable endpoint.</li> <li>The developer selects one or more interoperability rules and criteria (orchestration pattern) that are used for compliance testing.</li> <li>The developer specifies the endpoint of the GE for these rules to be tested against.</li> <li>The tool, based on the evaluation criteria and on the common models for the resources or GEs, provides as output to the user: an initial evaluation of the compliance of the GE with the specification.</li> </ol> <p>Infrastructure joiner:</p> <ol style="list-style-type: none"> <li>The user selects a set of interoperability orchestrations that match the behaviour they wish to achieve with their infrastructure i.e. am I a good candidate.</li> <li>The user executes these tests providing the concrete endpoints of the GEs as input to the tool.</li> <li>The tool provides as output an evaluation of where the infrastructure is and isn't compliant with a) individual FI-WARE specifications, b) overall Xifi federation behaviour. This report can be used to inform the infrastructure how they need to utilise Xifi adapters.</li> </ol>
Instances and Deployment	As per the Marketplace component
Issues & Notes	The tool is used as an aid to assess potential interoperability problems; it cannot fully verify interoperability or compliance.

### 7.1.9 Infrastructure Toolbox

Section	Description
Component name	Infrastructure Toolbox
Component Description and Functionalities	<p>This component provides the means to install the FI-WARE IaaS stack on a new node of the federation:</p> <ul style="list-style-type: none"> <li>hypervisor</li> <li>DCRM GE</li> </ul>

	<ul style="list-style-type: none"> <li>• Image Repository</li> <li>• SLM GE</li> <li>• Security system</li> <li>• Monitoring system</li> </ul> <p>This tool is used when a new infrastructure wants to join the federation. The user of this tool is the XIFI Consortium together with the infrastructure owner of the new infrastructure: they can decide what to install.</p> <p>The user can also select one or more adapters to be installed from the <i>Adapter Repository store</i> in case it is needed.</p> <p>In a first phase of XIFI, this tool can be implemented as something that provide an installation CD to be deployed on some VMs of the infrastructure.</p>
Interfaces Exposed	<p>GUI for allowing the users to package a set of tools/GE and create an installation CD.</p> <p>It will be integrated into the Marketplace component. Nevertheless it exposes also RESTful APIs to access its functionalities.</p>
Interfaces Requested	<ul style="list-style-type: none"> <li>• with the <i>Adapter Repository store</i> in order to get the adapters to be deployed</li> <li>• with the <i>GE Catalogue store</i> in order to get the GEs to be deployed</li> <li>• with the <i>Product Catalogue store</i> in order to get the products/tools to be deployed</li> </ul>
Behaviour	<ol style="list-style-type: none"> <li>1. The user (XIFI Consortium or infrastructure owner) selects a set of tools, GEs, adapters he wants to package</li> <li>2. The user creates an installation CD</li> <li>3. The user installs the CD on the infrastructure</li> </ol>
Instances and Deployment	As per the Marketplace component
Issues & Notes	

#### 7.1.10 Federation Service and Resource Manager

Section	Description
Component name	Federation Service and Resource Manager
Component Description and Functionalities	<p>This component is based on the Service manager GE and is responsible for managing the FI-WARE IaaS cloud stack software. For a description of SM GE, see [8]. The domain model that underpins the SM GE is the following:</p>  <pre> graph LR     Domain -- "0..*" --&gt; Project     Project -- "0..*" --&gt; VirtualAppliance[Virtual Appliance]     VirtualAppliance -- "0..*" --&gt; VirtualServer[Virtual Server]     VirtualServer --&gt; Volume     VirtualServer --&gt; ComputingFlavor[Computing Flavor]     VirtualServer --&gt; VirtualImage </pre>

	<p>This component is used by the XIFI Consortium in order to manage the virtual appliances and projects. Nevertheless it is used by other XIFI components in order to access the virtualization layer. Each time a new VM is created, the Federation Service and Resource Manager should automatically deploy on it all the components needed to manage it, like the <i>SDC client GE</i> and the <i>monitor probe GE</i>.</p> <p>Through this component and leveraging also on the DCRM GE [7] it should be possible to move a VM snapshot across different nodes.</p>
Interfaces Exposed	For the SM GE, see [8]. The GUI wrapper will expose the SM GE Restful API in a graphical manner. Nevertheless it exposes also RESTful APIs to access its functionalities.
Interfaces Requested	<ul style="list-style-type: none"> <li>For the SM GE, see [8].</li> <li>With the <i>Scalability Rules store</i> in order to get the scalability rules</li> </ul>
Behaviour	This component mimics the behaviour of the SM GE, see[8].
Instances and Deployment	The SOM part (see FI-WARE documentation) is deployed in high availability mode: two redundant instances located on two different <i>master</i> nodes of the federation. The SLM part is deployed on each node of the federation (one instance for each node).
Issues & Notes	

### 7.1.11 PaaS Manager

Section	Description
Component name	Paas Manager
Component Description and Functionalities	<p>This component implements the PaaS provisioning model and provides functionalities to deploy, undeploy and manage a software platform. It is based on the FIWARE PaaS GE [10] and SDC GE [9].</p> <p>This component will access the GE Catalogue in order to browse and select the relevant GEs to be installed and the Product Catalogue in order to get the needed COTS (Components Off The Shelf). It is generally used by a developer that wants to deploy a new customized software platform suitable for his needs, but can be used also by the XIFI Consortium together with the infrastructure owners in order to create a software platform offering access to some GEs in a SaaS model.</p> <p>The deployment strategy is based on some recipes as the ones used in Chef (currently SDC GE is based on Chef). This component uses SDC GE in order to deploy the products/GEs software and the Federation Service and Resource Manager component in order to deploy the virtual resources (VApp). The scalability/elasticity is also handled through the Federation Service and Resource Manager.</p> <p>For the functionalities offered by the PaaS and SDC GE, see the corresponding description on the FI-WARE wiki.</p>
Interfaces Exposed	A GUI integrated into the Marketplace will wrap the RESTful APIs offered by the PaaS and SDC GEs. Nevertheless it exposes also RESTful APIs to access its functionalities.

	For a detailed description of the PaaS GE APIs, see the FI-WARE wiki documentation [10].
Interfaces Requested	<ul style="list-style-type: none"> <li>with the Federation Service and Resource Manager</li> <li>with the <i>GE Catalogue store</i> in order to get the GEs to be deployed</li> <li>with the <i>Product Catalogue store</i> in order to get the products/tools to be deployed</li> </ul>
Behaviour	<ol style="list-style-type: none"> <li>Through the Marketplace portal, the user access the PaaS Manager</li> <li>The user browses the GEs and the Product catalogues and selects the GEs/products he wants to install (each GE/product should have its proper installation recipe)</li> <li>The user specifies the characteristics of the VMs/VApps where he wants to install</li> <li>The user creates a blueprint template specifying: <ul style="list-style-type: none"> <li>the number and characteristics of the application tiers</li> <li>mapping among products/GEs and these tiers</li> <li>scalability rules</li> <li>usage of private vs public IPs</li> <li>any specific and customized installation parameters</li> </ul> </li> <li>The user deploys the software platform and use it</li> </ol>
Instances and Deployment	As per the Marketplace component
Issues & Notes	It is not clear at the moment if it is possible to integrate in XIFI directly the GUI wrapper provided by FI-WARE on the PaaS GE.

### 7.1.12 Federated Security and Security Dashboard

Section	Description
Component name	Federated Security and Security Dashboard
Component Description and Functionalities	<p>This component offers security functionalities to the whole federation:</p> <ul style="list-style-type: none"> <li>identity management</li> <li>authentication (single sign on)</li> <li>authorization</li> <li>access control</li> <li>security proxy</li> <li>security monitoring</li> </ul> <p>It should provide capabilities to "federate" the "proprietary" security systems of each infrastructure present in XIFI. In particular the infrastructures IdMs and authentication systems should be unified by this component in order provide the users with a seamless access to the XIFI federation.</p> <p>It is composed by a "remote" instance handling authentication, access control, security proxy and security probes at the node level and interfacing the proprietary security systems, and a "centralized" instance offering security services (mainly authentication and security monitoring) to all the XIFI federated services. The central instances and all the remote ones should be grouped in a sort of "circle of</p>

	<p>trust".</p> <p>The security monitoring functionality allows to monitor the federation resources against security risks; it is provided to the users through a Security Dashboard integrated into the Marketplace component and it gets security monitoring data from the security probes installed on each node.</p> <p>This component is based on the FI-WARE IdM GE [13], Access Control GE [12] and Security Monitoring GE [11].</p>
Interfaces Exposed	<p>This component should support:</p> <ul style="list-style-type: none"> <li>• SAML</li> <li>• OAuth 2.0</li> <li>• OpenId</li> </ul> <p>The Security Dashboard GUI will be integrated into the Marketplace portal.</p>
Interfaces Requested	none
Behaviour	<ul style="list-style-type: none"> <li>• User log-in to XIFI Marketplace and is authenticated by the SSO functionality offered by this component (IdM GE)</li> <li>• User wants to use some resources present on a given node. The keys needed for accessing the APIs are provided by this component (Access Control GE)</li> <li>• User checks the security risks through the Security Dashboard (Security Monitoring)</li> </ul>
Instances and Deployment	<p>It will be deployed in a distributed way:</p> <ul style="list-style-type: none"> <li>• a remote instance on each node handling local authentication, authorization, access control, security proxy, security probing and allowing a loose coupling with the central federation (IdM GE and Access Control GE)</li> <li>• a central instance unifying and federating all the security systems present in the federated nodes in as sort of "circle of trust" (IdM GE) and comprising also the Security Dashboard.</li> </ul>
Issues & Notes	

### 7.1.13 Federation Monitoring

Section	Description
Component name	Federation Monitoring
Component Description and Functionalities	<p>This component provide an unified and federated monitoring of all the resources and services offered by the XIFI federation. This means that the monitoring data collected from each service/resource/VM will be processed, normalized on a common schema and eventually aggregated at the federation level providing an overview of the behaviour and performance of the Federation. Moreover the monitoring data are feeding other XIFI components like the SLA Management for calculating SLA violations and the Federation Service and Resource Manager for triggering scalability rules.</p> <p>This component is composed by a remote instance installed on each node of the</p>

	<p>federation and interacting directly with the proprietary monitoring systems (if any) and a centralized part handling the aggregation of the data from the different nodes at a higher level. It should be multi-tenant offering the possibility to assign different visibility to data from different services/resources.</p> <p>This component is based on the FI-WARE Monitoring GE [14] and Perfsonar [16Error! Reference source not found.].</p>
Interfaces Exposed	See the FI-WARE Monitoring GE specification [14] and Perfsonar [16].
Interfaces Requested	<ul style="list-style-type: none"> <li>This component should be able to get the data from the monitoring system already used by the infrastructures. It should at least support standard interfaces like SNMP, JMX and JDBC.</li> <li>with the <i>Federation Monitoring Data store</i> in order to store aggregated monitoring data (at federation level)</li> </ul>
Behaviour	<ul style="list-style-type: none"> <li>Raw data is collected for each node by the remote monitoring instance</li> <li>Raw data is normalized on a common schema for each node by the remote monitoring instance</li> <li>Normalized data is sent to the central monitoring instance for aggregation, calculation, check threshold violation etc</li> <li>The "elaborated" monitoring data can be visualized by the XIFI Consortium, the infrastructure owners and the end users according to their role and profile.</li> </ul>
Instances and Deployment	<p>It will be deployed in a distributed way:</p> <ul style="list-style-type: none"> <li>one remote instance for each node</li> <li>one centralized instance for the whole federation</li> </ul>
Issues & Notes	<ul style="list-style-type: none"> <li>How to integrate Perfsonar with Monitoring GE</li> <li>One instance of Monitoring GE per node? Then a "federated" instance?</li> </ul>

#### 7.1.14 SLA Management

Section	Description
Component name	SLA Management
Component Description and Functionalities	<p>Through this component the SLAs on the resources/services of the XIFI federation can be managed. In particular this component provide functionalities to:</p> <ul style="list-style-type: none"> <li>SLA definition</li> <li>SLA negotiation</li> <li>SLA monitoring</li> <li>Possible rebate</li> </ul> <p>This component is used by the XIFI Consortium together with infrastructure owners to define SLAs for their services and by the end users (developers) for monitoring of those SLAs. The component is multi-tenant meaning that different users have their own "space" for their own defined SLAs.</p>
Interfaces Exposed	This component exposes a GUI that will be integrated into the Marketplace portal. Nevertheless it exposes also RESTful APIs to access its functionalities.
Interfaces Requested	<ul style="list-style-type: none"> <li>with the <i>Federation Monitoring Data store</i></li> </ul>



Behaviour	<ol style="list-style-type: none"> <li>1. The infrastructure owners defines a SLA for a resource/set of resources</li> <li>2. The infrastructure owner and the developer (end user) negotiate the application of a SLA</li> <li>3. The SLA is monitored through the monitoring data collected</li> </ol>
Instances and Deployment	As per the Marketplace component
Issues & Notes	

### 7.1.15 HelpDesk

Section	Description
Component name	HelpDesk
Component Description and Functionalities	<p>This tool provides to the end user (developer, service provider or in general a user of the federation) the means for:</p> <ul style="list-style-type: none"> <li>• requesting support,</li> <li>• issuing a new ticket,</li> <li>• monitoring the status of the tickets</li> <li>• and, more generally, contact XIFI help desk.</li> </ul> <p>The XIFI help desk personnel uses the same tool to inform the users about the status of their tickets and provide information and support.</p> <p>This tool is multi-tenant in the sense that each user can see only the information that pertains to him.</p>
Interfaces Exposed	This component exposes a GUI that will be integrated into the Marketplace portal. Nevertheless it exposes also RESTful APIs to access its functionalities.
Interfaces Requested	none
Behaviour	This component is used in scenario UC-4 and its behaviour mimics the one present in the aforementioned scenario.
Instances and Deployment	As per the Marketplace component
Issues & Notes	

## 7.2 Federation Models

From the FedSM project [15], there are five basic federation models proposed. Although these concentrate mainly on simply *sell with and sell through* business models (i.e. they are commercially focused), they offer a reasonable starting point. A federation can be defined as *an organization within which smaller divisions have some degree of internal autonomy*. Three basic actors can be considered:

1. The user (i.e. anyone requiring the services or resources offered by the federation);
2. The federator (i.e. the individual or component controlling and/or managing the result of federating individual members); and
3. The federation member (i.e. an individual or component joining the federation and thereby offering their services / resources to anyone using the federation)



The federation model defines how the actors relate to one another. There are five basic models suggested by FedSM which include:

1. **Invisible Co-ordinator:** this is effectively a certification or validation authority.
  - The federator defines membership rules, and checks compliance
  - The federation member works to comply with the rules and seeks checks/certification from the federator
  - The user finds and engages with members via other channels
  - Examples: certification authority, franchises, etc
2. **Advisor:** an initial port of call to find appropriate federation members.
  - The federator advises federation members on how to promote their capabilities through federation
  - The federator advises users on where to find the capabilities they need
  - The users decide which federation members to engage with
  - After initial referral, interaction is between federation member and user
  - Examples: government help desk, Amazon Partners, etc
3. **Matchmaker:** providing a needs-to-capabilities matching service
  - The federator advises members on how to promote their capabilities through federation
  - The federation members decide what capabilities to offer and the associated terms and conditions
  - The federator matches requests from users to capabilities / offerings from federation members
  - The federator controls resource allocation
  - The federation members control the exploitation of resources and execution of services / applications
  - Examples: brokers, kayak.com
4. **One-stop-shop:** a federation of peers offering composite services
  - The “federator” is effectively the group of federation members collaborating with one another
  - The federator defines the services and rules of engagement
  - The federation members provide contributions in accordance with those rules
  - Users engage with federation members who in turn call on other federation members to fulfil the request(s)
  - Users pay the federation member who is the initial point of contact
  - Federation members bill one another for their contributions
  - Examples: airline code sharing, online train booking
5. **Integrator:** prime contractor, brokering services and handling all engagement
  - The federator defines the services and rules of engagement
  - The federation members provide contributions in line with those rules
  - Users engage with the federator to access the resources /services available
  - The federator controls resource allocation, billing, execution etc
  - The federation member bills the federator for their resources/services

In practical terms, these models can be distinguished in terms of two extremes (see following figure): a certification role only and complete and tight integration; as well as a middle path: a loose federation. The key really is how those roles relate to the nature of interactions between users and the federator and federation members.

## Relations between Actors

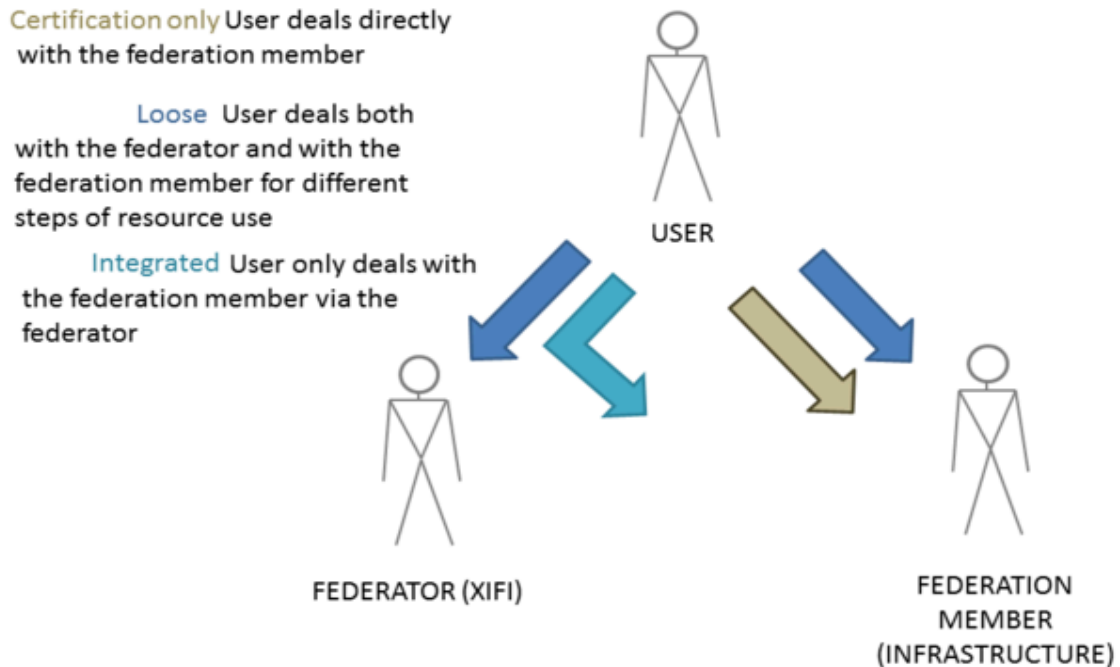


Figure 11. The three federation actors and their interactions.

### 7.2.1 Requirements

There are two main sources of requirements at this time:

1. Use Case projects
2. Initial XIFI nodes

In addition, the federation architecture (XIFI) is highly dependent on the functional capabilities of FI-WARE. As previously stated in this document, to address the other main sets of requirements (from the Use Cases and the XIFI nodes), a survey was conducted with each. For the purposes of federation models, here the authors reviewed the responses to specific questions about resource allocation, monitoring and contract management. They are summarised in the table below. In addition, the authors reviewed UC input to the “additional functions” questions, which related to concepts such as Help Desk, Data Backup, and so forth. For the initial draft federation model here, the authors have focused on those items which relate those UC project requirements to the Infrastructure responses.

Relationship between initial survey topics and functional areas within a federation		
Issuing and managing identity and other attributes to users	Identity management	UC
Authenticating/Verifying user identity and other attributes	Authentication	UC
Allocating my resources to match user requirements (i.e. a match-making service)	Allocation	
Informing users that my resources match their requirements, but leaving them to contact me to get	Resource discovery	

resource allocated (i.e. a recommendation service)		
Monitoring availability of my resources	Monitoring	UC
Negotiating SLA with users	SLA set up	
Mediating access to my resources once allocated (e.g. by allowing users to send requests indirectly via a XIFI portal or gateway)	Tracking	
Monitoring usage of my resources and generating accounting data for users coming through XIFI	Accounting	
Monitoring the security status of my resources	Security	

The infrastructure survey questions in this section relate approximately to nine federation functions: *Identity management, authentication, allocation, resource discovery, monitoring, SLA set up (i.e. initial negotiation of terms and conditions), tracking (i.e. access to resource after allocation), billing and security.*

The Use Case survey homed in on three of them (see previous figure): the need to provide access authorisation; the need for authentication; and a desire for operational logging and reporting (runtime monitoring). In addition, the authors assume that the user wishes handle as much through the federator as possible rather than being concerned about subtle differences in terms and conditions pertaining to individual resources and services provided by individual federation members. Taking the nine federation functions (see previous figure), the authors attempted to classify the appropriate federation model or models from the FedSM categories in the previous section with who (federator or federation member) should or could provide those functions.

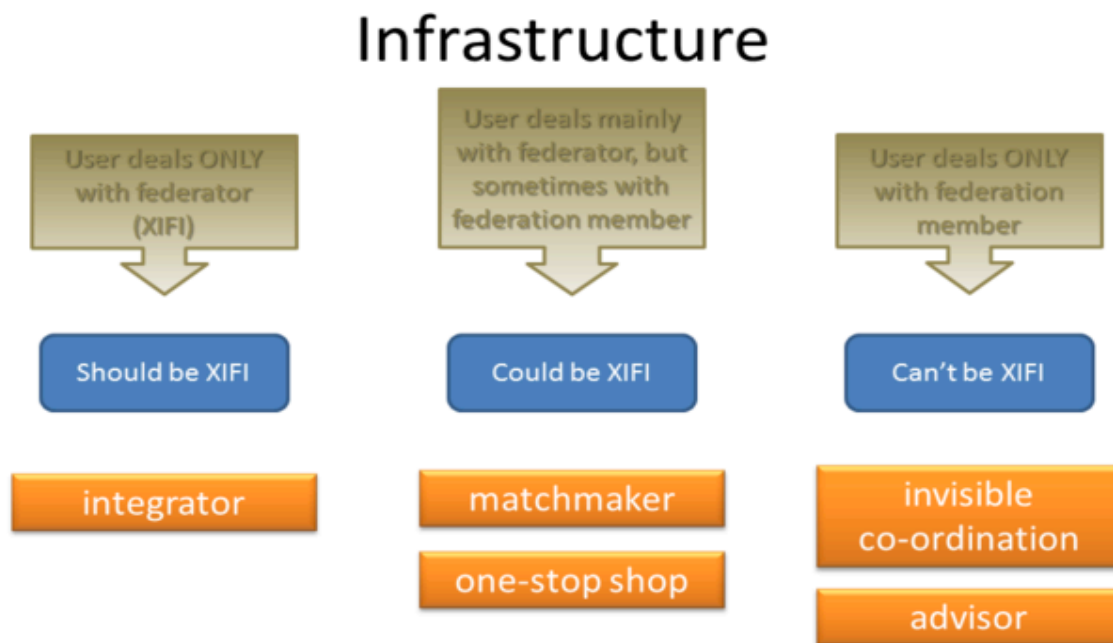


Figure 12. Summary of federation types and the distribution of functional responsibilities

As shown in the figure, if XIFI provides all functions (or at least the front end which the user interacts with), then:

1. The user deals only with XIFI (the federator) and
2. The best-match federation model would be integrator.

Conversely, if individual federation members insist on providing the function themselves, then:

1. The user deals only with the federation member, consulting the federator (XIFI) for information about who conforms with the overall functional patterns (i.e. FI-WARE) and
2. The best-match federation model would be either advisor or invisible co-ordination.

A hybrid approach would see most functions directly provided via a XIFI front-end, or indirectly. For now, this would imply:

1. The user usually deals with the federator (XIFI), and only occasionally with the federation member. For instance, if there are specific issues about data handling or specific requirements which are not generically used across the federation; and
2. The federation models could be either matchmaker or one-stop-shop.

The federator would directly provide some functions via, for instance, integration or interfacing pre-existing capabilities from the federation members (infrastructures). XIFI may also provide some functions indirectly via a XIFI Front Office.

Reviewing responses from the initial set of nodes indicate that the infrastructures differ slightly in which functions can or should be provided by XIFI and which must be retained by the node operator (in particular there are some issues on the Berlin infrastructure due to the management and access to the advances communication services like Sensor Networks, LTE Networks etc) it provides. But overall the One-Stop-Shop (or the Matchmaker) can be considered the federation model that can be applied to the XIFI federation.

Of course this is just a preliminary analysis, and in the future it should be further investigated (in T1.3 and in WP8).

## 8 CONCLUSIONS

In this document the authors provided an overview of XIFI concepts and objectives together with the definition of a methodology for gathering requirements from XIFI stakeholders. The preliminary results of the surveys on UC requirements have been presented highlighting the main requests coming from them. The five core nodes have been described in terms of hardware, virtualization services and other services they can offer focusing on the constraints they posed on the XIFI federation. From all this material, five core scenarios have been developed in order to describe the behaviour and the interactions of the most relevant use cases that can happen in XIFI. Finally, from the scenarios, the first draft of the architecture has been derived providing both a technical and a business view. The technical view gives the specification of a deployment model of the federation and the minimal set of constraints posed to an infrastructure that wants to join the XIFI federation. Moreover the list of the main architectural components together with their description and a diagram specifying their relationships are provided. The business view lists five possible federation models and, using the requirements gathered during the UC and infrastructure survey, tries to select one or two of them as applicable to XIFI.

## REFERENCES

---

1. XIFI Consortium, XIFI Description of Work.
2. National Institute of Science and Technology, The NIST Definition of Cloud Computing.. Retrieved 30 July 2013. <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>
3. HP, Seven design principles for building a converged cloud. Retrieved 30 July 2013. <http://www8.hp.com/h20195/v2/GetDocument.aspx?docname=4AA4-6524ENW>
4. A. Avizienis, J.C. Laprie, B. Randell, and C. Landwehr, Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 1, NO. 1, JANUARY-MARCH 2004.
5. FI-WARE Consortium, FI-WARE Architecture. Retrieved 30 July 2013. [https://forge.fiware.eu/plugins/mediawiki/wiki/fiware/index.php/FI-WARE\\_Architecture](https://forge.fiware.eu/plugins/mediawiki/wiki/fiware/index.php/FI-WARE_Architecture)
6. FI-WARE Consortium, Cloud Hosting Architecture. Retrieved 30 July 2013. [https://forge.fiware.eu/plugins/mediawiki/wiki/fiware/index.php/Cloud\\_Hosting\\_Architecture](https://forge.fiware.eu/plugins/mediawiki/wiki/fiware/index.php/Cloud_Hosting_Architecture)
7. FI-WARE Consortium, DataCenter Resource Management (DCRM)Open Specification. Retrieved 30 July 2013. <https://forge.fiware.eu/plugins/mediawiki/wiki/fiware/index.php/FIWARE.OpenSpecification.Cloud.DCRM>
8. FI-WARE Consortium, Service Manager GE Open Specification. Retrieved 30 July 2013. <https://forge.fiware.eu/plugins/mediawiki/wiki/fiware/index.php/FIWARE.OpenSpecification.Cloud.SM>
9. FI-WARE Consortium, Software Deployment and ConfigurationGE Open Specification. Retrieved 30 July 2013. <https://forge.fiware.eu/plugins/mediawiki/wiki/fiware/index.php/FIWARE.OpenSpecification.Cloud.SDC>
10. FI-WARE Consortium, PaaSGE Open Specification. Retrieved 30 July 2013. <https://forge.fiware.eu/plugins/mediawiki/wiki/fiware/index.php/FIWARE.OpenSpecification.Cloud.PaaS>
11. FI-WARE Consortium, Security Monitoring GE Open Specification. Retrieved 30 July 2013. <https://forge.fiware.eu/plugins/mediawiki/wiki/fiware/index.php/FIWARE.OpenSpecification.Security.SecurityMonitoring>
12. FI-WARE Consortium, Access Control GE Open Specification. Retrieved 30 July 2013. [https://forge.fiware.eu/plugins/mediawiki/wiki/fiware/index.php/FIWARE.OpenSpecification.Security.Access\\_Control\\_Generic\\_Enabler](https://forge.fiware.eu/plugins/mediawiki/wiki/fiware/index.php/FIWARE.OpenSpecification.Security.Access_Control_Generic_Enabler)
13. FI-WARE Consortium, Identity Manager GE Open Specification. Retrieved 30 July 2013. <https://forge.fiware.eu/plugins/mediawiki/wiki/fiware/index.php/FIWARE.OpenSpecification.Security.IdentityManagement>
14. FI-WARE Consortium, Monitoring GE Open Specification. Retrieved 30 July 2013. <https://forge.fiware.eu/plugins/mediawiki/wiki/fiware/index.php/FIWARE.OpenSpecification.Cloud.Monitoring>
15. FedSM Consortium, D3.1: Business models for Federated e-Infrastructures. Retrieved 30 July 2013. [http://www.fedsm.eu/sites/default/files/FedSM-D3.1-Business\\_models-v1.0.pdf](http://www.fedsm.eu/sites/default/files/FedSM-D3.1-Business_models-v1.0.pdf)



16. perfSONAR project, Technical Overview. Retrieved 30 July 2013.  
<http://www.perfsonar.net/overview.html>