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

eXperimental Infrastructures for the Future Internet

D1.4: Analysis of UC, Infrastructures and Enablers v2

Revision: v1.1

Work package	WP1
Task	T1.2
Due date	30/06/2014
Submission date	15/07/2014
Deliverable lead	Create-Net
Authors	Silvio Cretti (CNET), Federico Facca (CNET), Sean Murphy (ZHAW), Badia Philippe (Com4Innov), Aristi Galani (UPRC), Jonas Lindqvist (ACREO), Stefan Bouckaert (IMINDS), Rudolf Vohnout (CESNET), Miguel Egido (GOWEX), Georgios Kormentzas (Neuropublic), Yuriy Andrushko (BTH), Ioannis Igoumenos (UTH), Sándor Laki (WIGNER), Bartosz Belter (PSNC) Joaquin Iranzo Yuste (ATOS), Jose Gonzales (UPM)
Reviewers	Brian Pickering (IT-INN), Sean Murphy (ZHAW)

Abstract	This report continues the work started with deliverable D1.2 giving an up to date (at month 15 of the project) analysis of the high level requirements collected so far from the different stakeholders (both internal and external ones). Moreover a brief analysis of the 12 new infrastructures, selected during the XIFI Open Call, is provided in order to understand possible barriers for them to join FI-Lab through the federation managed by XIFI.
Keywords	Requirements, UC projects, FI-WARE, Infrastructures

Document Revision History

Version	Date	Description of change	List of contributor(s)
V1.0	02.07.2014	Version ready for internal review	Silvio Cretti (CNET) et al.
V1.1	15.07.2014	Final version	Silvio Cretti (CNET) et al.

Disclaimer

This report contains material which is the copyright of certain XIFI Consortium Parties and may only be reproduced or copied with permission in accordance with the XIFI consortium agreement.

All XIFI Consortium Parties have agreed to publication of this report, the content of which is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License[1].

Neither the XIFI Consortium Parties nor the European Union warrant that the information contained in the report is capable of use, or that use of the information is free from risk, and accept no liability for loss or damage suffered by any person using the information.

Copyright notice

© 2013 - 2015 XIFI Consortium Parties

Project co-funded by the European Commission in the 7th Framework Programme (2007-2013)		
Nature of the Deliverable:	R (Report)	
Dissemination Level		
PU	Public	✓
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to bodies determined by the XIFI project	
CO	Confidential to XIFI project and Commission Services	

[1]http://creativecommons.org/licenses/by-nc-nd/3.0/deed.en_US

EXECUTIVE SUMMARY

This document provides an up-to-date version of the deliverable D1.2 [1]. It aims in particular at consolidating the high level requirements collected so far from the different stakeholders (both internal and external) presenting a snapshot at month 15 of what is continuously updated in the online project tools (the wiki - http://wiki.fi-xifi.eu - and the Redmine - http://redmine.fi-xifi.eu).

External stakeholders that have been considered are mainly the Phase II UC projects and the FI-WARE project whereas internal stakeholders comprise: showcases developed within XIFI to demonstrate technical and business capacities offered by FI-Ops and FI-Lab; business work packages, that explore business models and business requirements for tools (i.e. FI-Ops), the federated platform for developers (i.e. FI-Lab) and its sustainability beyond FI-PPP; and infrastructure owners that, through XIFI, are becoming part of FI-Lab. This document lists also requirements on FI-WARE Generic Enablers and/or infrastructural cloud components (like the Cloud Portal and the PaaS Manager GE): in this case the objective is to keep track of the enhancements requested to FI-WARE components which are mainly due to the distributed and multi-regional nature of FI-Lab following the injection of XIFI infrastructures.

Since this is the first deliverable in WP1 after the finalization of the XIFI Open Call, it also gives a brief description of the twelve new infrastructures selected with the objective to verify potential barriers for them to join the federation.

The main result of the work described in this document is the updated set of high-level requirements. Some new requirements, coming from the different stakeholders, have been identified and added to the requirement list but they do not appear to affect in a significant way the federation architecture presented in D1.3 [3] and should fit well in the current architectural framework. Nevertheless a more detailed analysis, from an architectural point of view, of these new requirements will be presented in deliverable D1.5 and the possible impacts on the federation architecture will be evaluated.

TABLE OF CONTENTS

EXECUTIVE SUMMARY **3**
TABLE OF CONTENTS **4**
LIST OF TABLES **7**
ABBREVIATIONS **9**
1 INTRODUCTION **10**
1.1 Context, Objective and Scope of this Deliverable 10
1.2 Document Convention 11
1.3 Intended Audience and Reading Suggestions 11
2 NEW INFRASTRUCTURES DESCRIPTION **13**
2.1 iMinds iLabt.XiFi 13
2.1.1 Brief Description 13
2.1.2 Data Centre 13
2.1.3 Virtualization services 13
2.1.4 Other features 14
2.1.5 Services provided 14
2.1.6 Constraints imposed by this infrastructure on the federation 14
2.2 ICCLab ZHAW - Zurich University of Applied Science 14
2.2.1 Brief Description 14
2.2.2 Data Centre 15
2.2.3 Virtualization services 15
2.2.4 Other features 15
2.2.5 Services provided 15
2.2.6 Constraints imposed by this infrastructure on the federation 15
2.3 PSNC - Poznan Supercomputing and Networking Centre 15
2.3.1 Brief Description 15
2.3.2 Data Centre 16
2.3.3 Virtualization services 16
2.3.4 Other features 16
2.3.5 Services provided 16
2.3.6 Constraints imposed by this infrastructure on the federation 16
2.4 Neuropublic 17
2.4.1 Brief Description 17
2.4.2 Data Centre 17
2.4.3 Virtualization Services 17
2.4.4 Other features 17

2.4.5 Services provided 17
2.4.6 Constraints imposed by this infrastructure on the federation 17
2.5 CESNET 17
2.5.1 Brief Description 18
2.5.2 Data Centre 18
2.5.3 Virtualization services 18
2.5.4 Other features 18
2.5.5 Services provided 18
2.5.6 Constraints imposed by this infrastructure on the federation 18
2.6 TNS - Telecommunication Networks and integrated Services 19
2.6.1 Brief Description 19
2.6.2 Data Centre 19
2.6.3 Virtualization services 19
2.6.4 Other features 19
2.6.5 Services provided 20
2.6.6 Constraints imposed by this infrastructure on the federation 20
2.7 Com4Innov 20
2.7.1 Brief Description 20
2.7.2 Data Centre 21
2.7.3 Virtualization services 21
2.7.4 Other features 21
2.7.5 Services provided 21
2.7.6 Constraints imposed by this infrastructure on the federation 21
2.8 XIFI NFN - Nordic Federated Node 21
2.8.1 Brief Description 21
2.8.2 Data Centre 22
2.8.3 Virtualization services 22
2.8.4 Other features 22
2.8.5 Services provided 22
2.8.6 Constraints imposed by this infrastructure on the federation 22
2.9 XIFIBUR 22
2.9.1 Brief Description 22
2.9.2 Data Centre 23
2.9.3 Virtualization services 23
2.9.4 Other features 23
2.9.5 Services provided 24
2.9.6 Constraints imposed by this infrastructure on the federation 24

2.10 WIGNER 24
2.10.1 Brief Description 24
2.10.2 Data Centre 24
2.10.3 Virtualization services 25
2.10.4 Other features....25
2.10.5 Services provided....25
2.10.6 Constraints imposed by this infrastructure on the federation 25
2.11 NITOS - Network Implementation Testbed using Open Source platforms....25
2.11.1 Brief Description 25
2.11.2 Data Centre 26
2.11.3 Virtualization services 26
2.11.4 Other features....26
2.11.5 Services provided....27
2.11.6 Constraints imposed by this infrastructure on the federation 27
2.12 BTH CloudLab 27
2.12.1 Brief Description 27
2.12.2 Data Centre 27
2.12.3 Virtualization services 27
2.12.4 Other features....28
2.12.5 Services provided....28
2.12.6 Constraints imposed by this infrastructure on the federation 28
2.13 Recap of new infrastructures analysis and constraints 28
3 HIGH LEVEL REQUIREMENTS 29
3.1 UC Projects Requirements....29
3.1.1 FINESCE 29
3.1.2 FITMAN....30
3.1.3 FI-STAR 30
3.1.4 FI-SPACE 31
3.1.5 FI-CONTENT2....31
3.1.6 Concluding Remarks on UC Project Requirements....31
3.2 Internal Requirements....31
3.2.1 Showcases Requirements....32
3.2.2 Business/Socio-Economic Requirements 33
3.3 Requirements for FI-WARE....36
3.4 Requirement List 37
4 CONCLUSIONS 44
REFERENCES 45

LIST OF TABLES

Table 1: iMinds data centre 13
Table 2: iMinds virtualization services 13
Table 3: iMinds other features 14
Table 4: iMinds services provided 14
Table 5:ICCLab data centre 15
Table 6:ICCLab virtualization services 15
Table 7:ICCLab services provided 15
Table 8:PSNC data centre 16
Table 9:PSNC virtualization services 16
Table 10:PSNC services provided 16
Table 11:Neuropublic data centre 17
Table 12:Neuropublic virtualization services 17
Table 13:Neuropublic service provided 17
Table 14:CESNET data centre 18
Table 15:CESNET virtualization services 18
Table 16:CESNET services provided 18
Table 17:TNS data centre 19
Table 18:TNS virtualization services 19
Table 19:TNS other features 20
Table 20:TNS services provided 20
Table 21:Comm4Innov data centre 21
Table 22:Acreo data centre 22
Table 23:Acreo virtualization services 22
Table 24:Acreo services provided 22
Table 25:XIFIBUR data centre 23
Table 26:XIFIBUR virtualization services 23
Table 27:XIFIBUR other features 23
Table 28:XIFIBUR service provided 24
Table 29:WIGNER data centre 24
Table 30:WIGNER virtualization services 25
Table 31:WIGNER other features 25
Table 32:WIGNER services provided 25
Table 33:NITOS data centre 26
Table 34:NITOS virtualization services 26
Table 35:NITOS other features 26

Table 36:NITOS services provided 27
Table 37:BTH data centre 27
Table 38:BTH virtualization services 27
Table 39:BTH services provided 28
Table 40: FINESCE expectations 30
Table 41: FITMAN expectations 30
Table 42: FI-STAR expectations 31
Table 43:Socio-Economic requirement analysis 36

ABBREVIATIONS

FI-PPP	Future-Internet Private Public Partnership
FTTH	Fiber To The Home
GE	Generic Enabler
HPC	High Performance Computing
IaaS	Infrastructure as a Service
IdM	Identity Manager
IoT	Internet of Things
MD-VPN	Multi Domain – Virtual Private Network
NREN	National Research and Education Network
PaaS	Platform as a Service
QoE	Quality of Experience
QoS	Quality of Service
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SDN	Software Defined Networking
SDR	Software Defined Radios
SE	Specific Enabler
SFA	Slice-based Federation Architecture
SME	Small Medium Enterprise
UC	Use Case
VM	Virtual Machine
WP	Work Package
WSAN	Wireless Sensor and Actuator Network

© 2013 - 2015 XIFI Consortium Parties

1 INTRODUCTION

The XIFI project aims at supporting the creation of a community cloud[2] for European FI-PPP developers enabled by advanced FI infrastructure in Europe. By now, a first release on this community cloud is up and running and available at http://lab.fi-ware.org. FI-Lab serves the purpose of being the entry point for the developers engaging with FI-WARE (http://www.fi-ware.org) and FI-PPP (http://www.fi-ppp.eu) technologies.

FI-PPP is an ambitious programme by the European Commission part of the 7th Framework Programme aiming at exploring the potential of a common platform for Future Internet technologies to establish new business ecosystems. In this context, FI-WARE is the common platform for Future Internet technologies, envisioned by the FI-PPP.

XIFI project, in this context, supports:

- the deployment of FI-Lab,
- the enhancement of FI-WARE technologies to support the multi-node (or region using cloud traditional terminology) deployment of FI-Lab and
- the development of tools (FI-Ops) to support deployment and operation of FI-Lab nodes (or standalone FI-WARE instances).

Different users and stakeholders have different needs toward the three assets mentioned above. Deliverable D1.2 [1] presents a first round of these requirements that were collected at the early stages of the project. At this point in time, with first adopters using both FI-Lab and FI-Ops and a larger plethora of infrastructures part of the federation backing FI-Lab, we can better complete the picture of needs and collect feedbacks on previous requirements.

1.1 Context, Objective and Scope of this Deliverable

This deliverable aims at consolidating the high level requirements gathered until month 15 of the XIFI project. In general, the requirements collected pertain to functionalities offered by FI-Lab to developers, to federation functionalities supported by FI-Lab for the infrastructure owners, and to tools (FI-Ops) for supporting the operation of FI-Lab and infrastructures. At month 12, XIFI project started a new round of the requirement gathering process from the internal and external stakeholder with the following objectives:

- UC projects are our main clients at the moment and some of them have already started to use services and infrastructures provided by XIFI within FI-Lab. So now they are more familiar with the FI-Lab/FI-Ops offering and can provide useful and interesting hints on how to further develop and enhance the federation services and operation support tools.
- Internal stakeholders, like showcases developers (WP6) and business work packages (mainly WP8), are interested in providing new requirements from a perspective that encompasses not only the technical aspects but covers also the socio-economic ones to tackle sustainability of FI-Lab and the backing infrastructure federation.
- The number of infrastructures, that are going to be part of FI-Lab through the federation build by XIFI, increased as a result of the XIFI Open Call: twelve new infrastructures are progressively joining the federation. Checking their status and the possible constraints they

[2]"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"[Error! Reference source not found.].

have can be of great help for making the federation more interoperable and open to accommodate different kinds of infrastructures.

- FI-WARE is the main technology provider for FI-Lab and the work done in XIFI to extend FI-Lab capacity is so far the most important use case for FI-WARE Cloud Chapter and related Generic Enablers. The interaction between the two projects is very important for the success of the FI-PPP initiative and in this document these interactions and the information exchanged have been described in terms of requirements imposed by XIFI project on some of FI-WARE GEs and/or infrastructural components mainly related with the set-up of a cloud federation.

The procedure used to collect requirements from the different "sources" is explained in deliverable D1.1.1 [2]: for UC projects and FI-WARE we leveraged on the FI-PPP Architecture Board, on frequent virtual meetings and on the designation of some XIFI partners as "facilitators" in the case of UC projects. Moreover, the adoption by UC projects of the nodes and functionalities, offered by XIFI project through FI-Lab, simplified the interactions and helped to understand their real needs. Unfortunately not all the UC projects have already adopted FI-Lab as platform where to run their experiment and often the reason seems to be related to the needs of having a private cloud platform (for specific security and privacy issues)or a platform ready at the early stage of the project (an initial extensions of FI-Lab, including XIFI nodes and features, was up & running only from month 9, even though we have been provisioning standalone cloud capacity since month 6, for example to FI-Star).

The information and expectations gathered from the different "sources" have then been elaborated in order to verify if the needs are already covered by existing requirements, if they are within the scope of XIFI projects (see D1.1.1 [2] for a detailed definition of the federation build by XIFI, what its purpose and vision are and consequently what is in the XIFI project scope) and/or if new requirements are needed to fulfil them. Based on this analysis, carried out in Task 1.2, this document presented an up-to-date list of high-level requirements.

The derived list of high level requirements will then be considered in subsequent deliverables (in particular D1.5) in order to verify its impact on the FI-Lab architecture (in Task 1.3) and to extract detailed requirements on the different components (in WP2, WP3 and WP4): as usual the tracking and mapping process (see D1.1.1 [2]), that allows to keep an alignment between high level requirements, architectural components and detailed requirements, will be applied to this new list of requirements as well.

1.2 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.

1.3 Intended Audience and Reading Suggestions

The intended audience of this document comprises:

- Use Case projects in order to understand how their requirements have been addressed by XIFI project.
- FI-WARE project and platform for keeping into account the requirements imposed by XIFI project in order to enhance the functionalities of the FI-WARE GEs and infrastructural components to be deployed in FI-Lab.
- XIFI project partners involved in technical activities so as to have an overview of the current status of high level requirements collected so far from the different stakeholders: requirements of course will drive the design and implementation of the FI-Lab federated platform.

- All the XIFI project partners in order to have a common understanding of the objective and scope of the XIFI project: what is in the requirement list is in scope and what is not, at least at the moment, is out of scope.
- In general, any third party developer, interested in using FI-Lab and the federation behind it for experimentation, in order to have an understanding of what it can offer.

This document is divided into the following sections:

- **Section1** - this section - introduces the objectives and scope of the document.
- **Section 2** provides a brief description of the new infrastructures focusing on possible constraints or barriers to their integration into the federation.
- **Section3** describes the high level requirements identified so far and collected from different stakeholders:
    - UC projects
    - Internal stakeholders
    - The FI-WARE project

  Finally a complete list of all the high level requirements is provided.
- **Section 4** gives the conclusions of this deliverable providing a very preliminary analysis of the possible impact of the new requirements on the architecture and design of federation functionalities of FI-Lab and the operational tools to support infrastructure owners' part of the federation.

2 NEW INFRASTRUCTURES DESCRIPTION

This section provides a brief description of the twelve new infrastructures, selected through the Open Call, that are going to join the federation. For each infrastructure a brief description is provided together with the main characteristics of their data centre capacity, of the virtualization services, of other possible features not directly related with the data centre and of the services offered. When appropriate, possible constraints are highlighted.

2.1 iMinds iLabt.XiFi

Operated by: iMindsvzw (www.iminds.be/en)

2.1.1 Brief Description

The iMinds iLab.t technical testing facilities host multiple state-of-the-art technical testbeds and advanced testing equipment. The iLab.t technology centre is located in Gent, Belgium, and can in many cases be operated remotely. However, it is also possible to connect additional (third-party) equipment and/or integrate third party software into the testbeds.

The two most used generic testbeds in iLab.t today are the "Virtual Wall" and "w-iLab.t". In addition, an ambitious third experimentation environment, "Homelab" is being set up.

In this facility we will dedicate 8 servers to FI-Lab, but with the possibility of scaling up if needed.

2.1.2 Data Centre

Component	Description	Comment
Total Capacity	128 cores, 16 CPUs, 384GB RAM, 8TB storage	
Servers	8 servers (Supermicro)	
Per server capacity	2x 8cores, 2x Xeon e5-2650v2, 48GB RAM, 1TB hard disk	
Network	IPv4/IPv6 internet 1Gbps + dedicated 2Gbps to GEANT for AutoBAHN, point-to-point, SDN and openflow available if needed	

Table 1: iMinds data centre

2.1.3 Virtualization services

Component	Description	Comment
Hypervisor	XEN	
Cloud Manager	OpenStack, Emulab	
Base OS	Ubuntu 12.04 LTS	

Table 2: iMinds virtualization services

2.1.4 Other features

Component	Description	Comment
Virtual Wall	320 similar servers as above	accessible through SFA Federation and with international connectivity
w-iLab.t	Wifi and sensor testbed (200 nodes)	accessible through SFA Federation and with international connectivity
L3-L7 load generating equipment	Spirent Avalanche, test centre	

Table 3: iMinds other features

2.1.5 Services provided

Service	Description	Comment
Helpdesk	4 people available	
Monitoring	Internal Zabbix + Fed4FIRE monitoring dashboard	

Table 4: iMinds services provided

2.1.6 Constraints imposed by this infrastructure on the federation

1. IPv4 public address ranges are very limited, so IPv6 is preferred.
2. Bandwidth from commercial internet to iMinds is restricted to 200Mb/s; from iMinds to commercial internet bandwidth is 1Gb/s and with research internet also 1Gb/s.

2.2 ICCLab ZHAW - Zurich University of Applied Science

Operated by: Zurich University of Applied Science (www.zhaw.ch/en/zurich-university-of-applied-sciences.html)

2.2.1 Brief Description

The ICCLab at ZHAW runs a number of cloud computing deployments for research and experimentation as well as educational purposes. ICCLab is making some of its resources available to the XIFI project to enable it to integrate with FI-Lab and using this to promote the Future Internet vision within Switzerland. The ICCLab has resources split between one of the ZHAW Data Centres in Winterthur and an Equinix Data Centre in central Zurich.

2.2.2 Data Centre

Component	Description	Comment
Total Capacity	200 cores, 768 GB ram, 40TB disk	Target capacity
Servers	5 Lynx Calleo 1240s at present	Purchasing extra equipment - models TBC
Per server capacity	2*Intel E5620 (8 cores), up to 192 GB, 1 TB disk	
Network	1 Gbps NREN connectivity (SWITCH), pica8 for SDN support	

Table 5:ICCLab data centre

2.2.3 Virtualization services

Component	Description	Comment
Hypervisor	KVM	
Cloud Manager	Openstack	
Base OS	CentOS 6.x	

Table 6:ICCLab virtualization services

2.2.4 Other features

None.

2.2.5 Services provided

Service	Description	Comment
Monitoring	Nagios monitoring is used locally	

Table 7:ICCLab services provided

2.2.6 Constraints imposed by this infrastructure on the federation

No MD-VPN support provided by local NREN: an alternative solution is required.

2.3 PSNC - Poznan Supercomputing and Networking Centre

Operated by: Poznan Supercomputing and Networking Centre (www.man.poznan.pl/online/en/)

2.3.1 Brief Description

PSNC delivers all the resources required to integrate with FI-Lab. This includes network connectivity resources, as well as a subset of its own HPC/private cloud infrastructure. This infrastructure will be dedicated only to FI-Lab and not used for other purposes.

2.3.2 Data Centre

Component	Description	Comment
Total Capacity	34 CPUs (Intel Xeon E5345), 136 Cores, 34 GB RAM, 2TB external storage	CPU with Intel® Virtualization Technology (VT-x), storage from SAN (choice of FC/iSCSI/NFS/Lustre)
Servers	17 x (2x Intel Xeon, 16GB RAM, 1 Gbps Eth, 160 GB storage)	
Per server capacity	8 Cores, 2 GB RAM, 20+ GB storage/core	
Network	Juniper EX4300 with 48x1GE & 4SFP, 40 Gbps to PIONIER backbone, 2x 10 Gbps GÉANT network	GÉANT node is located in PSNC

Table 8:PSNC data centre

2.3.3 Virtualization services

Component	Description	Comment
Hypervisor	KVM	
Cloud Manager	OpenStack	
Base OS	any open-source OS can be supported	

Table 9:PSNC virtualization services

2.3.4 Other features

None.

2.3.5 Services provided

Service	Description	Comment
Monitoring	24/7 monitoring by Network Operation Center	
EduGAIN	The eduGAIN service is intended to enable the trustworthy exchange of information related to identity, authentication and authorisation between the GÉANT Partners' federations.	More information can be found on http://www.geant.net/service/eduGAIN/Pages/home.aspx

Table 10:PSNC services provided

2.3.6 Constraints imposed by this infrastructure on the federation

None.

2.4 Neuropublic

Operated by: Neuropublic, SA (www.neuropublic.gr).

2.4.1 Brief Description

A state of the art cloud infrastructure for added valued services mainly focusing on agricultural and e-commerce areas. The platform community already has more than 850.000 subscribers.

2.4.2 Data Centre

Component	Description	Comment
Total Capacity	120 Cores Intel VT-x, 264 GB RAM, 4 TB Disk	Target capacity
Servers	To be defined	
Per server capacity	To be defined	
Network	300Mbps Internet, 1 Gbps Internal Network, HP Openflow Switch	

Table 11:Neuropublic data centre

2.4.3 Virtualization Services

Component	Description	Comment
Hypervisor	KVM	
Cloud Manager	OpenStack	
Base OS	CentOS 6.x	

Table 12:Neuropublic virtualization services

2.4.4 Other features

None.

2.4.5 Services provided

Service	Description	Comment
Monitoring	Using Zabbix	

Table 13:Neuropublic service provided

2.4.6 Constraints imposed by this infrastructure on the federation

None.

2.5 CESNET

Operated by: CESNET, a.l.e. (www.cesnet.cz/?lang=en).

2.5.1 Brief Description

In the CESNET node the computing resources are optimized for performance per unit of price and physical space taken in the rack. These design goals led to the selection of SuperMicro'sFatTwin server family and the latest generation of CPUs from AMD. The RAM sizes were more than doubled compared to the minimal requirements set in the XIFI OpenCall proposal. Network-wise, the resources are connected straight to CESNET's core network over a dedicated 10G fibre link. Close proximity to an in-house GÉANT pop enables bandwidth-hungry applications to run in an efficient manner on this particular node. Local storage is provided by 10k SFF hot-swap drives deployed in a fully-redundant configuration.

2.5.2 Data Centre

Component	Description	Comment
Total Capacity	192 CPUs (Opteron 6344), 768 GB RAM, 8 TB disk space	
Servers	8x SuperMicro H8DGT (A+ 2122TG)	
Per server capacity	24 cores (2 sockets), 96 GB RAM, four hot-plug 10k drives, RAID10 for performance and reliability	
Network	Juniper EX4300-24T, SDN support, 10Gbps connection to CESNET's backbone and GÉANT	

Table 14:CESNET data centre

2.5.3 Virtualization services

Component	Description	Comment
Hypervisor	libvirt/KVM	
Cloud Manager	OpenStack	
Base OS	Scientific Linux 6.x (a RHEL clone)	

Table 15:CESNET virtualization services

2.5.4 Other features

None.

2.5.5 Services provided

Service	Description	Comment
Monitoring	Using Collectd and Nagios	

Table 16:CESNET services provided

2.5.6 Constraints imposed by this infrastructure on the federation

None.

2.6 TNS - Telecommunication Networks and integrated Services

Operated by: Laboratory of Telecommunication Networks and integrated Services (TNS), Department of Digital Systems, University of Piraeus (http://tns.ted.unipi.gr).

2.6.1 Brief Description

The TNS Node supports the execution of a great variety of experimentations, particularly in the areas of the IoT (Internet of Things) and WSAN (Wireless Sensor and Actuator Network) as well as advanced wireless access covering open WiFi/LTE access points and SDR (Software Defined Radios).

2.6.2 Data Centre

Component	Description	Comment
Total Capacity	116 Cores, 272 GB RAM, 2.3 TB Storage	
Servers	3 Dell r715/ 5 HP Proliant G6	
Per server capacity	16 Cores, 64 GB Memory, 5x250 GB / 4Cores, 16GB Memory, 1x160 GB	
Network	Gigabit Ethernet connectivity, Open-WRT enabled Routers with PantouOpenFlow extension	

Table 17:TNS data centre

2.6.3 Virtualization services

Component	Description	Comment
Hypervisor	OpenStack with KVM support	Hypervisor
Cloud Manager	OpenStack Cloud Manager (Folsom release) / OpenStack Quantum DevStack, OpenNebula	Cloud Manager
Base OS	Ubuntu 12.04 (LTS)	Base OS

Table 18:TNS virtualization services

2.6.4 Other features

Component	Description	Comment
WLAN Access Points	CISCO AIR-AP1131AG	
WLAN Bridges	CISCO AIR-AP1242G	
Open-WRT enabled Routers	Linksys WRT54GL	
SDR eNodeB and UE	Blade RF SDR	
3G modem with GPRS, EDGE, UMTS and HSPA support	Huawei	
WSAN Gateways	Arduino Mega 2560 Rev3, WaspMote	

Component	Description	Comment
	Gateways, Meshlium Gateway, Raspberry Pi Modules	
Sensor nodes	Motion detection sensor, Temperature sensor, Humidity sensor, Luminosity sensor, Hall sensor, Ultrasonic sensor, Pressure sensor, Accelerometer	
Actuators	Fan Cooler (emulates a cooling system), Lamp, Led, Stove (emulates a heating system)	

Table 19:TNS other features

2.6.5 Services provided

Service	Description	Comment
Authentication	Username/password	
Monitoring	HP Network Node Manager	
Helpdesk		

Table 20:TNS services provided

2.6.6 Constraints imposed by this infrastructure on the federation

None.

2.7 Com4Innov

Operated by: Association PlateformeTélécom(www.com4innov.com).

2.7.1 Brief Description

Through the infrastructure and the services of Com4Innov, the Association PlateformeTélécom make available, operates and provides infrastructure resources and unique skills to the market players whether they are industrials (SMEs, large enterprise or industrial groups) or researchers. Com4Innov is a mutualised environment providing the market with the means to develop and validate their technologies, applications or services in the domains of networks and mobile services of the future (4G/LTE/IMS), M2M (Machine to Machine) and communicating objects / smart devices for the future Internet of Things. These domains are complemented with computing and data hosting in place for our users.

2.7.2 Data Centre

Component	Description	Comment
Total Capacity	96 cores - 192 GB ram - Disk 2.7 TB	
Servers	3 servers: Dell Power Edge R820	
Per server capacity	32 cores - 64 GB ram - HDD 900 GB	
Network	Connectivity, SDN	

Table 21:Comm4Innov data centre

2.7.3 Virtualization services

None at the moment.

2.7.4 Other features

None.

2.7.5 Services provided

None.

2.7.6 Constraints imposed by this infrastructure on the federation

None.

2.8 XIFI NFN - Nordic Federated Node

Operated by: Acreo(www.acreo.se).

2.8.1 Brief Description

The testbed is an established infrastructure. It is a live network, with a large number of end users, connected via FTTH and LTE. Here services may be evaluated by end users, prototypes may be integrated into the test network, demonstrations and interoperability tests may be performed. Also, the traffic monitoring framework provides input to the knowledge base on user behaviour, traffic patterns and QoS/QoE analysis.

2.8.2 Data Centre

Component	Description	Comment
Total Capacity	120 cores, 320 GB ram, 6 TB disk	
Servers	5x PowerEdge R720, Intel Xeon E-26XX v2 Processors	
Per server capacity	24 cores, 64GB RAM, 1.2TB storage	
Network	1 Gbps, OpenFlow	

Table 22:Acreo data centre

2.8.3 Virtualization services

Component	Description	Comment
Hypervisor	KVM	
Cloud Manager	OpenStack	
Base OS	Ubuntu Server 14.04 LTS	

Table 23:Acreo virtualization services

2.8.4 Other features

None.

2.8.5 Services provided

Service	Description	Comment
Monitoring	Nagios	

Table 24:Acreo services provided

2.8.6 Constraints imposed by this infrastructure on the federation

None.

2.9 XIFIBUR

Operated by: GOWEX Wireless (http://www.gowex.com/en/)

2.9.1 Brief Description

XIFIBUR proposes the creation of a completely new node for the instantiation of FI-WARE and its future developments. This node will be created following the XIFI node minimal requirements in a first step, but does not end there. By acquiring and deploying cutting edge hardware elements, XIFIBUR will implement extensive capabilities for the future scalability of the node. This hardware will be deployed in the CTIC (Information and Communication Technologies Centre) already existing at the Spanish city of Burgos, which implements the most advanced features in terms of operations and safety.

2.9.2 Data Centre

Component	Description	Comment
Total Capacity	208 Cores, 416 GB RAM, 26 TB HDD	
Servers	13 x DELL PowerEdge M620	
Per server capacity	• CPU: 2 x Intel Xeon E5-2603v2 (16 cores per sleigh, 2,4GHz) • RAM: 4 x 8GB RDIMM, 1.333MHz, Low Voltage, Dual Rank • HDD: 2 x 1TB SATA 7,2K, 2,5Zoll • Controller: H310 • Network: Broadcom 57810-k dual port 10Gb	
Network	• Switch: 2 x Dell Force10 MXL 10/40 GbE 32 ports • Router: Cisco Router ASR 1001 • Firewall: SonicWall NSA 3500	

Table 25:XIFIBUR data centre

2.9.3 Virtualization services

Component	Description	Comment
Hypervisor	KVM	
Cloud Manager	OpenStack Grizzly	
Base OS	Ubuntu12.04 serv64bit/Ubuntu Serv 13.04	

Table 26:XIFIBUR virtualization services

2.9.4 Other features

Component	Description	Comment
Network	• 6 WIMAX nodes • 200 outdoor WIFI Access Points • 40 Municipal Buildings with indoor coverage • 20 interactive Bluetooth nodes	
Services	• Advanced video-surveillance systems • Real-time public buses fleet management • Public Bicycle service • Video-Conference system • Sensors in the scope of park maintenance	

Table 27:XIFIBUR other features

2.9.5 Services provided

Service	Description	Comment
Backup	DELL POWERVAULT	
Platform Supervisor	Nagios	
Platform Monitoring	CACTI	

Table 28:XIFIBUR service provided

2.9.6 Constraints imposed by this infrastructure on the federation

None.

2.10 WIGNER

Operated by: Wigner Research Centre for Physics, Budapest, Hungary (http://www.rmki.kfki.hu/en)

2.10.1 Brief Description

The Wigner Research Centre for Physics is one of the research centres of the Hungarian Academy of Sciences, covering various research areas of physics, high performance computing and networking. In 2013, Wigner established the Wigner Data Centre with an investment of EUR 30 million from the Hungarian Government. This data centre is now one of the most advanced infrastructures in Central and Eastern Europe, hosting the Tier-0 data centres infrastructure of CERN – the largest CERN site outside Geneva - and the cloud infrastructure of the Hungarian Academy of Sciences Big Data efforts. The Wigner Node consists of the required computational resources, and in addition access to ETOMIC infrastructures (http://www.etomic.org) including ETOMIC testbed, ETOMIC-SONoMA and ETOMIC-Network Measurement Virtual Observatory (nmVO).

2.10.2 Data Centre

Component	Description	Comment
Total Capacity	128 cores, 256 GB RAM, 10 TB disk	Shared disk connected with InfiniBand
Servers	SGI ALTIX ICE 8200XE; 16 blades (1 IRU) dedicated to XIFI	1 blade for controller
Per server capacity	8 cores per blade (2x Intel Xeon X5365 3.0GHz), 16 GB RAM per blade	Shared disk
Network	1 Gbps connectivity to GÉANT and the Internet through the Hungraian NREN; InfiniBand connection between blades and storage node	

Table 29:WIGNER data centre

2.10.3 Virtualization services

Component	Description	Comment
Hypervisor	KVM	
Cloud Manager	OpenStack Grizzly	
Base OS	Currently RHEL 6.2	Wigner bought extended SGI support. With SGI we examine how Ubuntu 12.04 LTS could be installed on ICE blades. If it can be done, we will use Ubuntu as host OS, if not, RHEL will be upgraded to the latest version supporting OpenStack Grizzly.

Table 30:WIGNER virtualization services

2.10.4 Other features

Component	Description	Comment
OpenWRT enabled devices	Planned, but not yet deployed.	
ETOMIC access	Access to ETOMIC testbed, SONoMA and nmVO	

Table 31:WIGNER other features

2.10.5 Services provided

Service	Description	Comment
Monitoring	Nagios or Ganglia	We will also examine how our SONoMA-Periodic monitoring tool could be integrated.

Table 32:WIGNER services provided

2.10.6 Constraints imposed by this infrastructure on the federation

None.

2.11 NITOS - Network Implementation Testbed using Open Source platforms

Operated by: NITLAB - University of Thessaly (http://nitlab.inf.uth.gr/NITlab/)

2.11.1 Brief Description

The NITOS testbed is an integrated testbed with heterogeneous facilities that focus on supporting experimentation-based research in the area of wired and wireless networks. NITOS is remotely accessible and open to the research community 24/7. It has been used by hundreds of experimenters all over the world. UTH and NITOS have participated in multiple experimentation driven EU projects.

2.11.2 Data Centre

Component	Description	Comment
Total Capacity	112 Cores, 224GB RAM, 3TB HDD	Scalable
Servers	7 Hp G8 blade Servers	HP ProLiant BL460C G8
Per server capacity	16 cores, 32GB RAM, 300GB HDD	
Network	Gigabit network connectivity through an openflow switch	Servers host 10G interfaces

Table 33:NITOS data centre

2.11.3 Virtualization services

Component	Description	Comment
Hypervisor	ESXi	Will be replaced by KVM Hypervisor
Cloud Manager	VSphere Client	Will be replaced by Openstack Software
Base OS	Any OS can be supported	Ubuntu, Windows, RedHat, etc

Table 34:NITOS virtualization services

2.11.4 Other features

Component	Description	Comment
NITOS Node Testbed	Nodes supporting multiple heterogeneous interfaces	
USRP - GNU Radios	SDR (Software Defined Radio)	
Mobile Nodes	Nodes moving around the space	Roomba robots, Android hand-held devices
WiMAXTestbed	Infrastructure supporting experimentation on WiMAX technology	
LTE Testbed	Infrastructure supporting experimentation on LTE technology	
Wireless Sensor Network	Deployment of sensors around urban and agro-field territories	
SDN Testbed	Openflow Switches and Controllers	

Table 35:NITOS other features

2.11.5 Services provided

Service	Description	Comment
Monitoring	OML Library	
Big Data support	MapReduce is used with a distributed and parallel algorithm	Hadoop case study

Table 36:NITOS services provided

2.11.6 Constraints imposed by this infrastructure on the federation

None.

2.12 BTH CloudLab

Operated by: BlekingeTekniskaHögskola - Blekinge Institute of Technology(http://www.bth.se/ENG)

2.12.1 Brief Description

The BTH CloudLab provides another extension of FI-Lab into Scandinavia, and in particular to the southern Swedish region of Blekinge. Moreover, CloudLab integrates BTH's renowned Network Performance Lab (NPL) into FI-Lab. In this way it enables current and future software developers (inside and outside Blekinge) to do test-driven development of their applications with regard to scalability and performance.

2.12.2 Data Centre

Component	Description	Comment
Total Capacity	64 cores (AMD-V), 256GB RAM, 2TB storage	Soon (2014 Q3) to be increased with additional 108 cores
Servers	2x PowerEdge R715	
Per server capacity	32 cores, 128GB RAM, 1TB storage	
Network	1Gbps, OpenFlow	

Table 37:BTH data centre

2.12.3 Virtualization services

Component	Description	Comment
Hypervisor	KVM	
Cloud Manager	OpenStack	
Base OS	Linux-based OS	

Table 38:BTH virtualization services

2.12.4 Other features

None.

2.12.5 Services provided

Service	Description	Comment
Monitoring	Network Performance Laboratory	

Table 39:BTH services provided

2.12.6 Constraints imposed by this infrastructure on the federation

None.

2.13 Recap of new infrastructures analysis and constraints

From the brief description of the twelve new infrastructures provided in the previous section, it appears clear that the constraints imposed on the federation are not so constraining and they do not prevent these new infrastructures from joining the federation (indeed this was expected because the new infrastructures have been selected through the XIFI Open Call) following a One-Stop-Shop or Integrator federation model (see D1.1.1 [2]). Moreover almost all the new partners plan to completely reserve to FI-Lab a part of their whole infrastructure buying new hardware and assuring in this way more freedom in managing the integration. Nevertheless some relevant topics deserve to be highlighted and considered in the set up and deployment of the federation:

1. Some infrastructures have pointed out that the local NREN is not able to provide the MD-VPN service and/or that the bandwidth or IP addresses availability is limited:
    - This is not a big limitation because a workaround has been developed in order to overcome the lack of MD-VPN service (see REQ-4 in section 3.4).
    - On the other hand the limited bandwidth/IP address availability can be managed giving a "slave" role to that infrastructure (see D1.1.1 [2]) because the bandwidth requested is less than for a “master” node.
2. Some infrastructures are already providing a monitoring system:
    - XIFI project could/should integrate that monitoring system in the federation monitoring system thanks to its adaptation layer (see D1.3 [3] and REQ-9 in section 3.4).
3. Some infrastructures can provide other features apart from the ones related to a "standard" data centre:
    - this may be of interest to support the needs of some UC projects or other developers requesting niche functionalities (see REQ-12 in section 3.4).

3 HIGH LEVEL REQUIREMENTS

3.1 UC Projects Requirements

In this second round of requirement gathering (the first round was summarized in D1.2 [1]) from UC projects, we applied the strategy and processes defined in D1.1.1 [2]. Moreover some dedicated virtual meetings with each UC project have been scheduled in order to directly discuss with them their needs and the plan to use FI-Lab and the infrastructures offered by XIFI project through FI-Lab. In preparation for these meetings, the UC projects have been provided in advance with the list of requirements already defined (see D1.2 [1] and D1.3 [3]) and, based on this set of requirements, they have been asked if they need to add more requirements or to modify something. Moreover each UC project has been asked a general question about their plan to use the XIFI facilities.

The results of this activity are not completely satisfactory because it has been really difficult to involve UC projects in the process and sometimes the information collected was not very relevant. In particular one UC (FI-CONTENT2) did not provide any information nor any availability to attend the virtual meetings. But this should not necessarily be interpreted in a negative way: maybe they are already comfortable with the current set of requirements and do not need to add more requirements or to submit new expectations. However, in general the UC projects that are already using XIFI facilities have demonstrated more reactivity in responding to our requests.

Hereunder the expectations collected from each UC project are reported, together with a brief analysis and the resulting new requirements elicited on XIFI project.

3.1.1 FINESCE

FINESCE is planning to use infrastructures offered by XIFI project through FI-Lab and for some trials (e.g. FINIESCE WP4) it is already using it (Trento node). In the following table the expectations gathered from FINESCE are reported together with a comment about their mapping onto requirements (either new or old ones):

Expectation	Comment[3]
Ability to migrate a VM and related data from a FI-Lab region to another	This is already addressed by the functionalities offered by the Cloud Management Platform adopted (OpenStack) even though it must be done following a manual process.
Support for setting up a private cloud	This is already addressed by REQ-13
Need of backup facilities	This is already addressed by REQ-7
Possibility to change the flavour of a VM	This is already addressed by the functionalities offered by the Cloud Management Platform adopted (OpenStack) even though it must be done following a manual process.
Each tenant should have assigned at least one public IP address; moreover a reverse proxy	This is a new requirement that will be added to the list of requirements as REQ-3.3 (see section

[3] Requirement identifiers, mentioned in this column, are present in Redmine and in D1.3. Nevertheless the complete list of requirements is presented in the table of section 3.4.

Expectation	Comment[3]
functionality should be provided by FI-Lab	3.4).
FI-WARE GE images should be available for deployment and some "complex" GEs (as Big Data) should be provided as SaaS model	This is already addressed by REQ-3
Monitoring system should provide the possibility to set thresholds and be alerted if some parameters of a VM cross the thresholds	This is a new requirement that will be added to the list of requirements as REQ-9.4 (see section 3.4).
When a new entry (resource, service or GE) becomes available in catalogue/marketplace, a notification should be sent to the registered users	This is a new requirement that will be added to the list of requirements as REQ-3.4 (see section 3.4).

Table 40: FINESCE expectations

3.1.2 FITMAN

FITMAN is planning to use FI-Lab and the infrastructures offered by XIFI project through FI-Lab and in fact it is already using it (Trento node). In the following table the expectations gathered from FITMAN are reported together with a comment about their mapping on requirements (either new or old ones):

Expectation	Comment[4]
Support for setting up a private cloud	This is already addressed by REQ-13
Need of backup and recovery facilities	This is already addressed by REQ-7
Need to support high availability and avoid single point of failure for the federation services	This is already addressed by REQ-6
Need to integrate in XIFI the FITMAN Catalogue providing access to FITMAN SEs	This is a new requirement that will be added to the list of requirements as REQ-2.2 (see section 3.4).

Table 41: FITMAN expectations

3.1.3 FI-STAR

FI-STAR is planning to use both private clouds and the infrastructures offered by XIFI project through FI-Lab. In particular they use a cloud hosted by the Technical University of Crete and the FI-Lab Berlin node. In the future, FI-STAR foresees the integration of the Crete node into FI-Lab. In the following table the expectations gathered from FI-STAR are reported together with a comment about their mapping on requirements (either new or old ones):

[4] Requirement identifiers, mentioned in this column, are present in Redmine and in D1.3. Nevertheless the complete list of requirements is presented in the table of section 3.4.

Expectation	Comment4
Support for setting up a private cloud	This is already addressed by REQ-13
Each tenant should have assigned at least one public IP address; moreover a reverse proxy functionality should be provided by XIFI	This is a new requirement that will be added to the list of requirements as REQ-3.3 (see section 3.4).
Need for non-conventional services like IoT and sensor network	This is already addressed by REQ-3.1 and REQ-12
Need to integrate in XIFI the FI-STAR Catalogue providing access to FI-STAR SEs	This is a new requirement that will be added to the list of requirements as REQ-2.2 (see section 3.4).

Table 42: FI-STAR expectations

3.1.4 FI-SPACE

At the moment FI-SPACE is using a dedicated could facility located in Turkey and equipped with OpenStack and FI-WARE technologies. They opted for this choice (instead of using the infrastructures offered by XIFI project through FI-Lab) in order to speed up the activities at the beginning of the project where infrastructures offered by XIFI project through FI-Lab were not yet up and running. In the future they plan to federate the Turkey node with FI-Lab and to consider a migration of some components of their environment on other FI-Lab nodes taking advantage of the capacity and geographically distributed nature of FI-Lab.

At the moment they are satisfied with the current set of requirements and do not have other needs to add. In particular avoiding single point of failure (REQ-6), supporting security (data protection and data privacy in particular - REQ-8) and monitoring of resources in term of performances and security (REQ-9.x) are the requirements most relevant for FI-SPACE that XIFI project needs to satisfy.

3.1.5 FI-CONTENT2

No further information provided during this round of requirement gathering. Nevertheless it appears that FI-CONTENT2 is planning to use the FI-Lab, in particular the FI-Lab node located in Lannion.

3.1.6 Concluding Remarks on UC Project Requirements

In the sections above, we have described the latest round of discussions with the UC projects. With the exception of FI-CONTENT2 (see above), the UC projects were positive in their responses. Two (FI-STAR and FI-SPACE), who had started to deploy on non-FI-Lab federated infrastructures because of scheduling issues, are planning to integrate those infrastructures into the FI-Lab, since they clearly recognise the benefits of doing so.

Of the sixteen expectations raised (FINESCE 8, FITMAN 4, and FI-STAR 4), ten have already been addressed by XIFI project, and the remaining six (some are duplicated) have been added to the new requirements being reported in this document.

3.2 Internal Requirements

Internal requirements come from two main sources:

- showcases (WP6) and
- business work packages (mainly WP8).

The showcase authors may have some interest in adding new requirements to the ones already specified in XIFI project in order to cover what their own showcases need; business work packages provide a non-technical vision of the project focusing on aspects relevant for enhancing sustainability, usability, exploitation, community building and can ask for features that are not yet covered by the current set of requirements.

As explained in D1.1.1 [2], the two aforementioned internal stakeholders have been surveyed in order to collect information of their needs and the material gathered has been analysed and compared to the current set of requirements (see D1.3 [3] for the latest consolidated list of requirements) in order to understand if new requirements need to be added.

The two sections hereunder describe the activities for showcases and business requirements respectively.

3.2.1 Showcases Requirements

Requirement gathering from showcases did not provide a lot of information because the range of requirements already considered in XIFI project covers in a satisfactory way the needs of these showcases (and to some degree this was expected since the showcases have been created in order to demonstrate the functionalities implemented by XIFI project in FI-Lab). Nevertheless four showcases proposed a set of new expectations to XIFI project mainly related to network controller functionalities. Hereunder the expectations provided are listed and analysed in order to understand if they are covered by current requirements or if new requirements should be added. For a detailed description of the different showcases, please refer to D6.2[4].

UC5 - Quality of Experience in NaaS

Expectations:

1. Support to QoS (queue priority management).
2. Ability to compute paths across federation with fault tolerance capability.
3. Integration between Network Controller and Monitoring System in order to check availability of the links.

Analysis:

- The first and second expectations are related to REQ-4 but a new detailed requirement addressing the Network Controller capabilities will be added (REQ-4.1 - see section 3.4).
- The third expectation is partially covered by REQ-9 but a new sub-requirement of REQ-4 will be added in order to request the Network Controller get monitoring data from the monitoring system and base its calculations on this data (REQ-4.2 - see section 3.4).

UC6: SDN traffic engineering and UC12: Migrating an existing experiment from FIRE to XIFI

Expectations:

1. Tenants should be able to manage the bandwidth rate limit (even though it will not be guaranteed)
2. Support to QoS (queue priority management).
3. Network Monitoring: basic measurements like latency, packet loss, throughput, jitter, etc should be collected on the federation network and provided to the Network Controller

Analysis:

- The first and second expectations are related to REQ-4 but a new detailed requirement addressing the Network Controller capabilities will be added (REQ-4.1 - see section 3.4).
- Third expectation is partially considered in REQ-9 but a new sub-requirement of REQ-4 will be added in order to request the Network Controller get monitoring data from the monitoring system and base its calculations on this data (REQ-4.2 - see section 3.4).

UC13: Augmented Virtual Tourist

Expectations:

1. Provide the possibility of attaching storage/volumes to a VM
2. Provide reverse-proxy functionality (possibly also a load-balancer) on a given public IP

Analysis:

- The first expectation is intrinsically provided by the Cloud Management Platform (OpenStack) adopted in FI-Lab so it is already considered/implemented.
- The second expectation is something raised also by other stakeholders mainly due to the lack of public IP addresses. Nevertheless since this is not explicitly described as a requirement, a new requirement will be added as sub-requirement of REQ-3 (REQ-3.3 - see section 3.4). On the other hand we think that the load-balancer functionality is something that should be implemented at application level rather than at "infrastructural level".

3.2.2 Business/Socio-Economic Requirements

This section provides an analysis of the business and socio-economic requirements collected during activities in the "business work packages" (in particular in WP8). The list of socio-economic requirements has been already commented on D1.3, but here the analysis aims at understanding if and how these requirements are applicable to the federation created by XIFI to extend FI-Lab (taking into account the XIFI project scope and vision elaborated in D1.1.1 [2]) and if these business requirements highlight some uncovered area by the current set of requirements: in this case new requirements will be added to XIFI project.

The analysis is presented in the table below where the first column provides the business/socio-economic requirement identifier, the second column describes the requirement, the third column maps the business requirement on a XIFI requirement (either a requirement already present in the requirement list or a new one) and the forth column elaborates on the requirement and on the mapping. All this information is present also on Redmine site (http://redmine.fi-xifi.eu).

Note - Four new requirements have been added thanks to this analysis on business and socio-economic requirements: REQ-4.1 and REQ-4.2 on network controller functionalities, REQ-10.1 on community building and REQ-15 on energy consumption monitoring. See section 3.4 for the complete list of requirements.

SE Req. Id	Socio-Economic Req. Description	Related XIFI Req.	Comment
SE_Req1	Users want a common look and feel when they access XIFI resources from anywhere at any time, to be able to personalise their entry point, but receive the same levels of service irrespective of where they store data and/or run experiments.	REQ-3	Covered by REQ-3 (only personalization is at the moment not considered).
SE_Req2	Resources should be accessible from any geographic location, signing in once and gaining access everywhere. The same operational standards should be maintained irrespective of access device or location.	REQ-3, REQ-6, REQ-8	Already covered by REQ-3, REQ-6, REQ-8. The second sentence of this requirement ("The same operational standards should be maintained irrespective of access device or location.") is not applicable to the federation developed by XIFI as far as access network is concerned: for example XIFI project cannot be responsible of the bad performances experiences if a user access it through a non appropriate channel (like an 56 Kb/s modem). Nevertheless as far as connectivity among nodes is concerned, the requirement is covered by the current federation capacities.
SE_Req3	To maintain trust, users should be kept informed of any and all activities, including faults and potential failures, when using the facilities	REQ-9, REQ-9.1, REQ-9.2, REQ-9.3	This requirement is supported by REQ-9, REQ-9.1, REQ-9.2 and REQ-9.3. Detailed analysis of what can be seen by which user type is provided in the detailed requirements of the Federation Monitoring component(s).
SE_Req4	Users want the same high-speed access irrespective of access location; they should be served with the same levels of QoS and QoE at all times	REQ-3, REQ-6, REQ-8	See SE_Req2
SE_Req5	The Community around XIFI should include all relevant actors and stakeholders, including the XIFI federation and federation members themselves; all should be encouraged to share knowledge and support. Community building and maintenance is very significant.	REQ-10, REQ-10.1	This is not only a technical requirement. From a technical point of view this is related to REQ-10 that can be further expanded to request the set up of tools enabling the community building. REQ-10.1 has been added to the requirement list in order to address this topic.
SE_Req6	Users will inevitably carry out	REQ-3,	It is related with the possibility to

SE Req. Id	Socio-Economic Req. Description	Related XIFI Req.	Comment
	experiments across multiple domains. They want to collaborate and share experience (see SE_Req5), but they will also use resource as fits them.	REQ-4, REQ-5, REQ-10.1	create an experimentation environment with resources belonging to different domains/regions. In this context it is related with REQ-3, REQ-4 and REQ-5. It is also partially related with REQ-8 (support to single sign on and federation of identities guarantee the coverage of this requirement as far as security aspects are concerned) and REQ-10.1 (collaboration and sharing of user experience).
SE_Req7	XIFI should keep stakeholders informed of overall progress, using some form of appropriate, targeted continuous self-validation	REQ-9, REQ-10.1	Covered by REQ-9 and REQ-10.1 as far as the technical matter is concerned. REQ-10.1 has been added as new requirement (see also SE_Req5).
SE_Req8	XIFI should be able to connect to other resources on demand and on an ad hoc basis as dictated by the requirements of users. This involves technical as well as commercial relationships to be enabled.	REQ-2, REQ-3.1, REQ-14	This requirement is not completely in the scope of XIFI project: the aim of XIFI project is mainly to provide a community cloud, together with other non-conventional services, for developers to experiment. Connecting to resources outside XIFI could be considered as explained in the requirement REQ-14. Moreover, the requirement REQ-3.1 covers the case of non-conventional services and REQ-2 addresses the configuration of any new resource joining the federation.
SE_Req9	In protecting personal as well as experimental data, XIFI needs to provide appropriate controls and auditability.	REQ-8, REQ-9.2	Covered by REQ-8 and REQ-9.2. See also comment in SE_Req3.
SE_Req10	The direct and broader communities around XIFI need careful management: understanding who they are, what motivates them and how best to communicate with them is essential for XIFI's success.	REQ-10, REQ-10.1	See SE_Req5.
SE_Req11	The participation of indirect actors and/or stakeholders should be considered (see also SE_Req5).	-	At the moment of writing, no information/requirements from "indirect stakeholders" is available.
SE_Req12	Network traffic between and within sites should be monitored, and be able to be managed. Users may	REQ-4, REQ-4.1, REQ-4.2,	Related to REQ-4 and REQ-9. Moreover two new requirements (REQ-4.1 and REQ-4.2) are added to

SE Req. Id	Socio-Economic Req. Description	Related XIFI Req.	Comment
	want to know and/or manage and control network traffic.	REQ-9	the requirement list in order to completely fulfil this request.
SE_Req13	XIFI should allow for up and down scaling of resource (i.e. planned configuration change) as well as the temporary, dynamic allocation of resource during execution (to cater for unforeseen requirement increase or decrease). Users may not be able to size their system requirements accurately, but would still expect them to run.	REQ-3.2	Addressed by REQ-3.2.
SE_Req14	XIFI Users should be able to run innovative and environmentally relevant experiments, connecting to 3rd party services if necessary (see SE_Req8), as well as expecting federation resources to be managed sustainably and efficiently.	REQ-15	See SE_Req8. Nevertheless a new requirement related to energy measurement can be added (REQ-15).
SE_Req15	As part of the federation as an environmentally sustainable entity (see SE_Req14), all resources and facilities should be sharable across all users under appropriate terms.	REQ-3, REQ-3.1, REQ-3.2	Covered by REQ-3, REQ-3.1 and REQ-3.2.
SE_Req16	XIFI should provide failover and recovery capabilities. Users expect continued operation as well as data integrity.	REQ-6, REQ-7	Covered by REQ-6 and REQ-7.
SE_Req17	XIFI needs to encourage participation, and complementing the knowledge sharing of the community (see SE_Req5) by providing training and context-specific help functionality. Users want support in preparation as well as during the use of the federated facilities.	REQ-10	The need to provide user support and training is already covered by REQ-10. For the rest, this requirement is out of scope of the XIFI project technical activities.

Table 43: Socio-Economic requirement analysis

3.3 Requirements for FI-WARE

The collaboration with the FI-WARE project has been carried on following the process described in D1.1.1 [2]. Close collaboration is especially needed in areas where XIFI project is intensively using the FI-WARE technology in order to build the infrastructure federation and extending FI-Lab:

- Cloud Management Platform (IaaS Management)

- Cloud Portal for accessing cloud functionalities
- PaaS Manager
- IdM and Security in general

The first topic has been well addressed in the first months of the XIFI project whereas the other three have been elaborated in more detail in the second part of the first year of the project. The findings of this analysis resulted in some functionalities not covered by the original components/GEs provided by FI-WARE. For this reason, a set of requirements has been identified as necessary. Such requirements have implications on the development of the cloud capabilities (e.g. Cloud Portal, PaaS Manager) in FI-WARE: these requirements have been formalized in the XIFI project and FI-WARE component backlogs (i.e. the backlogs of the software components involved):

1. Multi Region support: a user entering the cloud portal should be able to change the cloud region to which he is connected; moreover a user should be able to deploy virtual machines in different regions.
2. Ability to register a new region: a new infrastructure, willing to join the federation, should be registered in the cloud portal (either manually or automatically) as a new region.
3. Multi region blueprint support: a user should be able to create blueprint templates with tiers in different regions.
4. New role definition: since FI-Lab becomes a federation of infrastructures, at least the role of "administrator of a region/infrastructure" and of "administrator of the federation" (federation manager) should be defined. Moreover a user can be limited to access only a subset of the regions of the federation.
5. High Availability of “federation” services: security functionalities, like Identity Manager, Access Control and Security Proxy, but also other federation functionalities like the Cloud Portal should be offered in high availability so as to prevent any single point of failure.
6. Identity Federation: identity federation should be supported by the IdM using protocols like SAML (Security Assertion Markup Language). In this way identities, defined on the FI-Lab and/or pre-defined (locally) on the infrastructures, can be federated.

3.4 Requirement List

This section summarizes in a table the list of all the high level requirements gathered and defined so far. As usual in XIFI project, this is just a snapshot of the requirement list at month 15 of the project, whereas the continuously updated list is provided on Redmine (http://redmine.fi-xifi.eu**)**. The following table provides a requirements identifier and a title, a requirement description, the origin of the requirement (either XIFI internal or UC projects), the stakeholders that are mainly affected by the requirement (Infrastructure Owners, Developers) and the mapping to the five XIFI use cases scenarios described in D1.1.1 [2]. The requirement identifier is composed by one or two numbers: in the case of two numbers this means that the requirement is a sub-requirement of another requirement. **New requirements are highlighted in bold**.

Again an up to date list and the detailed information about the mapping of each of these high level requirements to detailed software component requirements (user stories and requirements defined for each software component) is provided in Redmine (http://redmine.fi-xifi.eu**)**.

Req. Id & Title	Description	Origin	Stakeholder[5]	Use Case
REQ-1 - Tools to set-up a new infrastructure	Provide tools to support the minimal set up of new infrastructures joining the federation starting from bare metal to an up & running federation node where software enabling cloud computing, monitoring and security functionalities has been (almost) automatically installed.	XIFI Internal	Infrastructure Owners	UC-1
REQ-2 - Registration process for joining the federation	Define the registration and validation process and tools for an infrastructure willing to join the federation. The process should include registration of services (e.g. OpenStack), resources (servers, storage), configuration and management of resource provisioning (e.g. definitions of quotas, roles, security rules, super-user identities).	XIFI Internal	Infrastructure Owners	UC-1
REQ-2.1 - Registration of conventional and non conventional services	Conventional services (related to software modules and GEs running in a data centre) and non-conventional ones (not directly related to a data centre like antennas, sensor networks etc.) can be registered in a catalogue and provided to the FI-Lab users.	XIFI Internal	Infrastructure Owners	UC-1
REQ-2.2 - Registration/Integration of third party resource catalogues	Provide the possibility to integrate/register third party catalogues where specific services and/or enablers (Specific Enablers) can be published and advertised. For example UC projects Specific Enabler catalogues can be integrated in FI-Lab.	UC Projects	Infrastructure Owners	UC-1
REQ-3 - Set up of development environments	FI-Lab should provide a marketplace/portal where the users can access FI-Lab offer, search and reserve resources and services, provided by the FI-Lab federated nodes, in order to create their own development environments. Services and resources can be provisioned and accessed through a SaaS or PaaS model transparently with respect to the node they belong to or the site where they are located.	XIFI Internal, UC Projects	Developers, Infrastructure Owners	UC-2
REQ-3.1 - Non-conventional services	In the FI-Lab marketplace also "non-conventional" services (like sensor network, LTE network etc) can be advertised. Their reservation and the negotiation of their usage could be also conducted "manually" contacting directly	XIFI Internal, UC Projects	Developers	UC-2

[5] Here we are considering the most relevant XIFI Stakeholders from an architectural perspective.

Req. Id & Title	Description	Origin	Stakeholder[5]	Use Case
	the infrastructure owner.			
REQ-3.2 – Support scalability	Scalability and elasticity of the virtualized development environments should be supported.	XIFI Internal, UC Projects	Developers	UC-2
REQ-3.3 - Public IP address and reverse-proxy functionality	Due to the potential high number of users and number of virtual machines on the FI-Lab federation and due to the fact that the number of public IP addresses available is limited, it is recommended that: • at least one public IP address is assigned to each tenant • a reverse-proxy functionality is requested so as to be able to reach many private addresses using a single IP address.	XIFI Internal, UC Projects	Developers, Infrastructure Owners	UC-2
REQ-3.4 - Notification of new entries in the FI-Lab marketplace	When a new entry (resource, service or GE) becomes available in FI-Lab catalogue/marketplace, a notification should be sent to the registered users.	UC Projects	Developers	UC-2
REQ-4 - Network configuration	Support network set up and configuration inside the FI-Lab federation in order to provide the requested network resources (bandwidth, cross-infrastructure interconnectivity, private connectivity among infrastructures) using technologies like MD-VPN (Multi Domain - Virtual Private Network) and SDN (Software Defined Networking).	UC Projects	Developers, Infrastructure Owners	UC-2
REQ-4.1 - Network Controller functionality	A Network Controller functionality based on SDN and offering 1. support to QoS: tenants should be able to choose among different service levels (e.g. Gold, Silver, Bronze) predefined in FI-Lab (without service interruption). Each level defines maximum bandwidth and/or traffic prioritization. In particular, the traffic entering a node should be prioritized with at least the following possibilities: • prioritization of incoming traffic among different tenants • prioritization of incoming	XIFI Internal	Developers, Infrastructure Owners	UC-2

Req. Id & Title	Description	Origin	Stakeholder[5]	Use Case
	traffic related to a single tenant according to the destination VM • prioritization of incoming traffic related to a single tenant according to the sources (e.g. IP address, Source VM if in a different FI-Lab node). 2. path computation 3. (nice to have) selection of predefined network topologies should be provided.			
REQ-4.2 - Network Controller functionalities based on monitoring data	Network Controller should be able to access monitoring data in order to base on it the network configuration functionalities like evaluation of link availability and calculation of the best end to end path.	XIFI Internal	Developers, Infrastructure Owners	UC-2
REQ-5 - Regions Availability	Allow services and resources to be located in different regions so as to: • guarantee location constraints: content and data can be subject to geographical and legal restriction about where they can be stored and processed. • support low network latency.	UC Projects	Developers	UC-2
REQ-6 - No Single Point of Failure	In order to avoid a single point of failure, FI-Lab should provide services as high availability: federation level FI-Lab services and tools (like Cloud Portal, Resource Catalogue, Help Desk, Security System) should be provisioned in high availability.	XIFI Internal, UC Projects	Developers, Infrastructure Owners	UC-2
REQ-7 - Backup and Recovery	FI-Lab should support backup and recovery indirectly through data replication and snapshot storage. This means that FI-Lab allows data replication and snapshot storage on its community cloud but it is responsibility of the developer to arrange his/her services/applications so as to take advantage of these features. Only in specific circumstances and on-demand a traditional backup service can be arranged.	UC Projects	Developers	UC-2
REQ-8 - Security	Security and Privacy services like: • authentication and authorization,	XIFI Internal,	Developers, Infrastructure	UC-2

Req. Id & Title	Description	Origin	Stakeholder[5]	Use Case
	• single sign on, • identity federation, • data protection, • data privacy, • network security, • security monitoring and auditing (see also REQ-9.2) should be provided.	UC Projects	Owners	
REQ-9 - Monitoring and SLA Management	FI-Lab should provide monitoring of: • network devices • end to end network connectivity • servers (both physical and virtual) and • services in order to gather data for Fault Management, Performance Management and SLA Management. Monitoring data should be collected either directly by FI-Lab services or gathered through an infrastructure proprietary monitoring system.	XIFI Internal, UC Projects	Developers, Infrastructure Owners	UC-5
REQ-9.1 - Federation Monitoring	Monitoring data should be aggregated and shown to the end user (having grants to see it) at the federation level through the use of a graphical user interface or a dashboard.	XIFI Internal, UC Projects	Developers, Infrastructure Owners	UC-5
REQ-9.2 - Security Monitoring	FI-Lab should monitor possible security attacks or threats in order to be able to react promptly.	XIFI Internal, UC Projects	Developers, Infrastructure Owners	UC-5
REQ-9.3 – Logging and Accounting	Activities like: • provisioning/de-provisioning of services • start/stop of VM • other user activities should be logged.	XIFI Internal, UC Projects	Developers, Infrastructure Owners	UC-5
REQ-9.4 - Set up threshold and alerts on monitoring data	The user should be able to set up thresholds on data collected by the monitoring system from virtual machines and services. Moreover alerts can be configured in case of threshold violation.	UC Projects	Developers	UC-5
REQ-9.5 SLA Management	Service availability should be monitored and considered in SLA. Moreover VM and/or service performances can be considered in SLA.	XIFI Internal, UC Projects	Developers, Infrastructure Owners	UC-5
REQ-10 - Help	Facilities should be provided for handling	UC	Developers	UC-4

Req. Id & Title	Description	Origin	Stakeholder[5]	Use Case
Desk and Tutoring	requests coming from end users, experiencing issues with FI-Lab, and/or from infrastructure owners that want to join the FI-Lab federation. Tutoring material and other initiatives like webinars should be provided.	Projects		
REQ-10.1 Set up of tools for enabling community building around XIFI	Tools that enable and ease the set up of a FI-Lab community should be provided: • social networks • blog • wiki • support and problem tracking	XIFI Internal	Developers	UC-4
REQ-11 - System Administration and Configuration Management	FI-Lab should provide tools for handling operations of the infrastructures federated like starting up and shutting down the relevant federation services, putting an infrastructure under maintenance for a period of time, modifying configuration parameters like quotas assigned to the users, security rules related the resources, network configuration (see also REQ-4).	XIFI Internal	Infrastructure Owners	UC-5
REQ-12 - Special hardware	Hardware different from that associated with a classical data centre, like GPU, sensor networks, mobile networks, large storage, should be provided.	UC Projects	Developers	UC-2
REQ-13 - Private Clouds	FI-Lab should provide support to build a private cloud: a user willing to create his own private cloud should be able to use some FI-Lab services (see REQ-1) in order to set it up. Moreover other FI-Lab services, like monitoring or security, can be used to manage this private cloud.	UC Projects	Infrastructure Owners	UC-3
REQ-14 - Special facilities	FI-Lab should provide support for integration with facilities and features offered by infrastructures related to specific domains (like smart hospital, smart factory, smart logistics, smart media). The integration can be pursued at different levels (ranging from completely private cloud - see REQ-13 - to interconnected infrastructures where only some FI-Lab services are exercised to – where feasible - completely federated infrastructures that become part of FI-Lab federation).	UC Projects	Infrastructure Owners	UC-3
REQ-15 - Energy	It would be nice if FI-Lab can install in its data centres power meters in order to	XIFI Internal	Infrastructure Owners	UC-5

Req. Id & Title	Description	Origin	Stakeholder[5]	Use Case
consumption measurement in data centres	monitor the energy consumption. This information can then be further analysed and can provide the first baseline for an improvement of the energy footprint.			

4 CONCLUSIONS

After the first deliverable of this series (D1.2 [1]), this document provides a snapshot at month 15 of the high level requirements gathering process from different sources:

- XIFI Internal:
  - showcases (WP6)
  - business work packages (WP8)
  - new infrastructures joining the federation after the Open Call
- Phase II UC projects

Moreover an analysis of the current FI-WARE technologies (infrastructural components and GEs mainly related with the setup of a cloud federation) and a comparison with the XIFI project needs has generated a set of requirements towards FI-WARE.

The process and methodology adopted to collect this information from different sources is well described and established in D1.1.1 [2] and has been applied to the activities reported in this document. The information collected has then been analysed, taking into account the XIFI project objectives, vision and scope, in order to extract new high level requirements for XIFI. The results of all this work are reasonably good in the sense that we were able to collect relevant information and expectations from each stakeholder and finally were able to provide a consolidated list of requirements in section 3.4. Nevertheless sometimes the interaction with some stakeholders, in particular the UC Projects, was not simple and as fruitful as expected and provided only a minimal set of information useful for XIFI project: as expected the UC projects that are already using the facilities, offered by XIFI through FI-Lab, have been the most active in providing new expectations. The collaboration between XIFI project and UC projects should be further investigated and probably not only at project level but more generally at the FI-PPP programme level.

Regarding the analysis of the twelve new infrastructures, we could conclude that there are not any relevant barriers that prevent them to join the federations and the few constraints imposed are already taken into account in the current architecture.

Overall few requirements have been added during this second round of requirement gathering. Moreover the new requirements are not so “substantial” and in most cases just clarify better (or detail) requirements already collected: this means that the requirement framework presented in the previous deliverables (D1.2 and D1.3) is still valid.

The list of requirements presented in section 3.4 can now be considered almost stable and we do not expect many other high level requirements to be added in the future. This means that the next architectural deliverable (D1.5) can provide also a well consolidated federation architecture model, stable for the rest of the project timespan. Indeed a very preliminary analysis of the new requirements from an architectural and design point of view does not point out any relevant changes to the current version of the high level architecture: surely some impacts on the design and implementation of specific components like:

- network controller,
- monitoring system and
- marketplace/catalogue

should be taken into account, but the overall framework can still be considered as valid and flexible enough to accommodate also the new requirements. This means that no big changes are expected to the architectural framework.

REFERENCES

[1] XIFI Deliverable D1.2: Analysis of UC, Infrastructures and Enablers v1

[2] XIFI Deliverable D1.1.1: XIFI Core Concepts, Requirements and Architecture Draft

[3] XIFI Deliverable D1.3: Federated Platform Architecture v1

[4] XIFI Deliverable D6.2: XIFI Showcases Demonstrators v1

© 2013 - 2015 XIFI Consortium Parties