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

eXperimental Infrastructures for the Future Internet

D6.1: XIFI Showcases Design V1

Revision: v.0.18

Work package	WP6
Task	Task 6.1, Task 6.2, Task 6.3, Task 6.4
Due date	31/12/2013
Submission date	17/02/2014
Deliverable lead	THALES
Authors	Jérémie Leguay (THALES), Gérard Nguengand (THALES), Pascal Bisson (THALES), Federico Michele Facca (CREATE-NET), Giuseppe Cossu (CREATE-NET), Massimo Vecchio (CREATE-NET), Davide Dalle Carbonare (ENG), Laura Pucci (ENG), Leonardo Villani (ENG), Thierry Milin (ORANGE), Boris Moltchanov (TI), Andrew Mackarel (HEANET), Susana Gonzalez Zarzosa (ATOS), Matthias Baumgart (DT), Panos Trakadas (SYNELIXIS), Fernando López Aguilar (TID), Ivan Biasi (TN), Stefano Modafferi (IT-INN).
Reviewers	Joaquin Iranzo Yuste (ATOS), Brian Pickering (IT-INN).

Abstract	This document describes thirteen (13) showcases developed in XIFI to demonstrate some of the unique features and services introduced by the XIFI federation. The main goal of these showcases is to exemplify the benefits of XIFI to the Future Internet community and help the communication and exploitation activities to advertise our outcomes. Finally, the presented showcases represent a valuable means to provide an internal validation of the outcomes of the XIFI technical work packages and infrastructure deployment.
Keywords	Future Internet, Showcases, XIFI Federation, Training material.

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-Non Commercial-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 describes the showcases developed in XIFI to demonstrate the specific features and services introduced by the XIFI federation. The main goal of these showcases is to highlight the benefits introduced by XIFI for the Future Internet (FI) community and to help the communication (i.e. WP9) and exploitation activities (i.e. WP10) to advertise our outcomes. Thus, each showcase targets one or more FI stakeholders to demonstrate the unique features and services introduced by the XIFI federation.

To facilitate the production of training material out of each showcase and the organization of related training (i.e. WP7), the XIFI consortium has defined most of the showcases to be small scale and requiring self-contained development. Moreover, the presented showcases represent a useful instrument to provide internal assessment of the outcomes of the XIFI technical work packages (i.e. WP1, WP2, WP3 and WP4) and of the infrastructure deployment (i.e. WP5). Finally, all the showcases will be deployed on the XIFI Community Cloud and will be accessible through the Future Internet Laboratory (FI-Lab), contributing to the promotion of the overall FI-PPP results to the wider FI community.

As said, each showcase will target one or more specific stakeholders (namely, infrastructures owners and operators, technology providers, developers and end users / adopters, to mention few of them) with the aim of showing how to benefit from XIFI. To this end, this document describes

- four showcases related to the deployment of new services on top of the XIFI Federation,
- three showcases focused on the performance of the XIFI Federation,
- four showcases dealing with the benefits for XIFI infrastructures, and
- two showcases presenting how XIFI can be used with complementary infrastructures.

TABLE OF CONTENTS

EXECUTIVE SUMMARY **3**
TABLE OF CONTENTS **4**
LIST OF FIGURES **6**
LIST OF TABLES **7**
ABBREVIATIONS **9**
1 INTRODUCTION **11**
2 XIFI SHOWCASES **13**
3 SHOWCASES ON XIFI NEW SERVICE DEPLOYMENT **15**
3.1 UC1: E-Health in a Smart City Environment 15
3.1.1 Showcase description 15
3.1.2 Technical description 17
3.1.3 Release plan 20
3.2 UC2: 3-tier GE deployment on multiple sites 20
3.2.1 Showcase description 20
3.2.2 Technical description 21
3.2.3 Release plan 22
3.3 UC3: SE registering and deployment 23
3.3.1 Showcase description 23
3.3.2 Technical description 24
3.3.3 Release plan 25
3.4 UC4: Marketplace services 26
3.4.1 Showcase description 26
3.4.2 Technical description 28
3.4.3 Release plan 29
4 SHOWCASES ON XIFI INFRASTRUCTURE PERFORMANCE **30**
4.1 UC5: Quality of Experience in NaaS 30
4.1.1 Showcase description 30
4.1.2 Technical description 31
4.1.3 Release plan 33
4.2 UC6: SDN traffic engineering 33
4.2.1 Showcase description 33
4.2.2 Technical description 34
4.2.3 Release plan 35
4.3 UC7: Monitoring QoS in the Node 36
4.3.1 Showcase description 36

4.3.2 Technical description 37
4.3.3 Release plan 38
5 SHOWCASES ON THE BENEFITS FOR XIFI INFRASTRUCTURES 39
5.1 UC8: Join the XIFI federation 39
5.1.1 Showcase description 39
5.1.2 Technical description 40
5.1.3 Release plan 41
5.2 UC9: Federated Login 42
5.2.1 Showcase description 42
5.2.2 Technical description 44
5.2.3 Release plan 45
5.3 UC10: Security monitoring 45
5.3.1 Showcase description 46
5.3.2 Technical description 46
5.3.3 Release plan 47
5.4 UC11: GE monitoring 48
5.4.1 Showcase description 48
5.4.2 Technical description 49
5.4.3 Release plan 50
6 SHOWCASES ON INNOVATION PATHWAY 51
6.1 UC12: Migrating an existing experiment from FIRE to XIFI 51
6.1.1 Showcase description 51
6.1.2 Requirements 53
6.1.3 Release plan 53
6.2 UC13: Augmented Mobile Tourist 54
6.2.1 Showcase description 54
6.2.2 Technical description 56
6.2.3 Release plan 57
7 CONCLUSIONS 58
REFERENCES 59

LIST OF FIGURES

Figure 1: The XIFI Stakeholder diagram. 11
Figure 2:UC1 description. 16
Figure 3: Architecture of the Berlin node. 17
Figure 4: UC1 architecture. 19
Figure 5: Datacentre interconnection. 21
Figure 6: App developer at the main page of the Maketplace. Available infrastructures are shown and there are also some GE suggestions such as top rated and newest enablers. 27
Figure 7: The app developer is also able to gather some detailed information about the different infrastructures. 28
Figure 8: Quality of Experience in NaaS. 31
Figure 9: XIFI infrastructure and advanced networking functionalities. 34
Figure 10: Statistics example. 37
Figure 11: ITBox Deployment Schema. 40
Figure 12: "Ask for Service" Use Case. 43
Figure 13: XIFI Login. 44
Figure 14: Overview of monitoring architecture in XIFI federation. 49
Figure 15: the OFERTIE Architecture. 52
Figure 16: Experiment Architecture. 53
Figure 17: Example. 55

LIST OF TABLES

Table 1: Summary of the selected showcases. 14
Table 2: UC1 Summary table. 15
Table 3: UC1 actors, roles and benefits summary. 16
Table 4: UC1 FI-WARE GEs. 18
Table 5: UC1 Self developed parts, SEs. 18
Table 6: UC2 Summary table. 20
Table 7: UC2 FI-WARE GEs. 22
Table 8:UC2 Self developed parts, SEs. 22
Table 9: UC3 Summary table. 23
Table 10: UC3 actors, roles and benefits summary. 24
Table 11: UC3 FI-WARE GEs. 25
Table 12: UC3 Self developed parts, SEs. 25
Table 13: UC4 Summary table. 26
Table 14: UC4 actors, roles and benefits summary. 27
Table 15: UC4 FI-WARE GEs. 29
Table 16: UC4 Self developed parts, SEs. 29
Table 17: UC5 Summary table. 30
Table 18: UC5 actors, roles and benefits summary. 31
Table 19: UC5 FI-WARE GEs. 32
Table 20: UC5 Self developed parts, SEs. 32
Table 21: UC6 Summary table. 33
Table 22: UC6 actors, roles and benefits summary. 34
Table 23: UC6 FI-WARE GEs. 35
Table 24: UC6 Self developed parts, SEs. 35
Table 25: UC7 Summary table. 36
Table 26: UC7 actors, roles and benefits summary. 36
Table 27: UC7 FI-WARE GEs. 38
Table 28:UC7 Self developed parts, SEs. 38
Table 29: UC8 Summary table. 39
Table 30: UC8 actors, roles and benefits summary. 40
Table 31: UC8 FI-WARE GEs. 41
Table 32: UC8 Self developed parts, SEs. 41
Table 33: UC9 Summary table. 42
Table 34: UC9 actors, roles and benefits summary. 43
Table 35: UC9 FI-WARE GEs. 45

© 2013 - 2015 XIFI Consortium Parties

Table 36: UC9 Self developed parts, SEs. 45
Table 37: UC10 Summary table. 45
Table 38: UC10 actors, roles and benefits summary. 46
Table 39: UC10 FI-WARE GEs. 47
Table 40: UC10 Self developed parts, SEs. 47
Table 41: UC11 Summary table. 48
Table 42: UC11 actors, roles and benefits summary. 49
Table 43: UC11 FIWARE GEs. 50
Table 44: UC11 Self developed parts, SEs. 50
Table 45: UC12 Summary table. 51
Table 46: UC12 FI-WARE GEs. 53
Table 47: UC12 Self developed parts, SEs. 53
Table 48: UC13 Summary table. 54
Table 49: UC13 actors, roles and benefits summary. 55
Table 50: UC13 FI-WARE GEs. 56
Table 51: UC13 Self developed parts, SEs. 56

ABBREVIATIONS

3G	Third generation
ABNO	Application-based Network Operations
API	Application Programming Interface
AR	Augmented Reality
BoD	Bandwidth on Demand
CPU	Central Processing Unit
DC	Data Centre
DCRM	Data Centre Resource Management
DDoS	Distributed Denial of Service
DEM	Data centre and Generic Enablers
E2E	End to End
FI	Future Internet
FIRE	Future Internet Research and Experimentation
GB	Gigabyte
GE	Generic Enabler
GPS	Global Positioning System
GUI	Graphical User Interface
HDD	Hybrid Drive
IaaS	Infrastructure as a Service
IdM	Identity Management
IDS	Intrusion Detection System
IP	Internet Protocol
IPv6	Internet Protocol version 6
ITBox	Infrastructure Toolbox
KVM	Kernel-based Virtual Machine
LTE	Long Term Evolution
LTS	Labelled transition system
M2M	Machine to Machine
MMPORG	Massive(ly) Multiplayer Online Role-Playing Game
MS	Media Server
NAM	Network Adapter Module
NaaS	Network as a Service
NCL	Nested Context Language
OAuth	Open Authentication
PaaS	Platform as a Service

© 2013 - 2015 XIFI Consortium Parties

PC	Personal Computer
PCE	Path Computation Element
PPP	Public-Private Partnership
PoI	Point of Interest
PS	Proxy Server
PXE	Preboot eXecution Environment
QoE	Quality of Experience
QoS	Quality of Service
RAM	Random Access Memory
RT	Real-time
RTC	Real-time communication
SAML	Security Assertion Markup Language
SDC	Software Deployment and Configuration
SDN	Software Defined Networking
SE	Specific Enabler
SIEM	Security Information and Event Management
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SM	Software Management
SSH	Secure Shell
SSO	Single Sign On
UC	Use Case
UGC	User Generated Content
UI	User interface
UMTS	Universal Mobile Telecommunications System
VM	Virtual Machine
VoIP	Voice over IP
VPN	Virtual Private Network
XIMM	XIFI Infrastructure Monitoring Middleware

© 2013 - 2015 XIFI Consortium Parties

1 INTRODUCTION

This deliverable presents a preliminary set of showcases that aims at demonstrating the XIFI capabilities to support Future Internet (FI) scenarios leveraging on FI Infrastructures, FI-WARE Generic enablers (GEs) and Use Case (UC) project Specific Enablers (SEs).

The main goal of these showcases is to exemplify the benefits of XIFI to the FI community and help the communication (i.e. WP9) and exploitation activities (i.e. WP10) to advertise our outcomes. Briefly, all the showcases cover one or more stakeholders identified in WP9 (and depicted in Figure 1) in collaboration with the other Work Packages, demonstrating specific features, tools, procedures and services introduced by the XIFI federation. Among the different stakeholders, the showcases primarily focus on: Developers (that leverage on XIFI infrastructure and technology provided through XIFI to build FI application and services); Technology Providers (that can leverage on XIFI infrastructure to deliver their GEs and SEs to Developers in a distributed fashion and taking advantage of FI facilities, such as Sensor Networks or 4G Antennas); Infrastructure Owners and Operators (that may want to join XIFI federation or to take advantage of FI-Ops tools for their infrastructure); and finally End Users / Adopters (that can experiment some domain specific application leveraging on FI-PPP technology build in the context of XIFI showcases).

Figure 1: The XIFI Stakeholder diagram[2].

[2] The up-to-date diagram is available at the following link: https://www.fi-xifi.eu/about-xifi/stakeholders.html

In particular, the showcases will show how XIFI can provide operational, as well as technical, benefits for potential UC trial application stakeholders and XIFI federation infrastructures, and they will be used to promote XIFI to both communities. The XIFI consortium has identified, planned and defined showcases that will be small-scale and thus require self-contained development, in order to facilitate the production of training material out of them and the proper organization of related training (i.e. WP7). This is particularly important for any stakeholder approaching XIFI, who would like to become familiar and exploit the unique capabilities and features that XIFI can offer in the shortest timespan.

Showcases are also a way to provide an internal validation of the outcomes of the XIFI technical work packages (i.e. WP1, WP2, WP3 and WP4) and of the infrastructure deployment (i.e. WP5). All the showcases will be deployed on the XIFI Community Cloud and accessible through the Future Internet Laboratory (FI-Lab), contributing to the promotion of overall FI-PPP results to the wider FI community.

Each showcase targets specific stakeholders and shows how XIFI can benefit them. In particular, the subset of the envisioned target stakeholders and how XIFI can benefit them are following:

- Developers and technology providers. For example, showcases supporting these categories of stakeholder focus on showing how:
    - multi-node services can be used and deployed on XIFI;
    - multi FI facility services can be used and deployed on XIFI;
    - advanced networking capacities among XIFI nodes can be used;
    - SEs can be deployed on XIFI;
    - services can be selected among XIFI nodes according to QoS requirements;

XIFI and FIRE together support an innovation process from early research experimentation on FIRE through to scalable business trials in the FI-PPP using XIFI;

- Infrastructure owners. For example, showcases supporting this category of stakeholders focus on showing how:
    - it is possible to install XIFI Cloud Services with a few clicks onto a bare-metal infrastructure;
    - it is possible to join XIFI federation;
    - it is possible to take part in the XIFI community;
    - XIFI provides access to new users and supports new business models.

2 XIFI SHOWCASES

To ease the description of all the showcases included in this deliverable and improve its readability and comprehension, the showcases have been preliminarily grouped into four main classes (namely, XIFI new service deployment, XIFI infrastructure performance, benefits for XIFI infrastructures and innovation pathway).

- **XIFI new service deployment**: these showcases aim at demonstrating how to develop and deploy new services on the XIFI infrastructure. The goal is to show developers how to easily develop, deploy and validate complex and distributed FI applications leveraging on the XIFI infrastructure.
- **XIFI infrastructure performance**: this group of showcases aims at demonstrating how the XIFI federation can provide interesting features for quality of service (QoS), whose parameters depend on the infrastructure capacity underlying the service (such capacity can be decomposed into computational, storage and networking capacity).
- **Benefits for XIFI infrastructures:** this group of showcases aims at demonstrating the services and opportunities that XIFI federation provides to infrastructures taking part into XIFI federation.
- **Innovation pathway**: the goal of this group of showcases is to demonstrate the value of XIFI as a test facility, federated with and complementing other facilities (e.g. FIRE) by plugging the gap between research, experimentation and real-world business deployment.

Along these four directions, that match the 4 tasks of WP6, we have pragmatically selected a total of 13 showcases (summarized in Table 1) that can be realistically implemented within the time frame of the project (also considering that the XIFI federation is being setting-up while the showcases are being developed). Then, in the following sections, each showcase and its corresponding overall domain area (eg. users, XIFI performance) are briefly summarized. Moreover, for each of them, a detailed implementation plan, together with a list of requirements and the planned release schedule are provided.

Showcase group	Short name	Showcase name	Value	Stakeholders
XIFI new service deployment	UC1	e-Health in a Smart City Environment	Shows the inclusion of non-conventional resources for a GE and SE-based critical service.	Developers, Technology providers, End Users / Adopters
	UC2	3-tier GE deployment on multiple sites	Demonstrates remote, distributed deployment of components within a 3-tier architecture.	Developers, Technology providers, Infras. owners & operators Public authorities
	UC3	SE registering and deployment	Shows interactions with the Marketplace to make SEs available, including related SLA and accounting activities.	Technology Providers and infrastructure owners
	UC4	Marketplace services	Shows how to find resource and enablers, and how to experiment with deployment options.	Developers Technology providers Infras. owners & operators

XIFI infrastructure performance	UC5	Quality of Experience in NaaS	Shows how to Use standard approaches to support QoE via QoS management.	Developers Technology providers Infras. owners & operators
	UC6	SDN traffic engineering	Shows how to ensure appropriate QoS between and within nodes.	Developers, Technology providers, Infrastructure owners & operators
	UC7	Monitoring QoS in the Node	Shows hot to evaluates the QoS on the node and select the best node where deploying a given GE, to maximize the efficiency of any experimentation.	Developers Infras. owners & operators
Benefits for XIFI infrastructures	UC8	Join the XIFI federation	Shows how to add a new node to the XIFI federation.	Infras. owners & operators
	UC9	Federated Login	Shows trust relationships between XIFI and external entities allowing SSO with credentials from any such trusted entity.	Developers Infras. owners & operators
	UC10	Security monitoring	Demonstrates the implementation and the use of suitable security features to detect and manage various different threats.	Infras. owners & operators
	UC11	GE monitoring	Demonstrates the installation simplicity and added value arising from gathering GE monitoring data on federation level.	Developers Infras. owners & operators
Innovation pathway	UC12	Migrating an existing experiment from FIRE to XIFI	Shows how to migrate an existing experiment from an experimental context to XiFi. Demonstrate SDN management.	Developers
	UC13	Augmented Mobile Tourist	Demonstrates the service deployment of a traditional "vertical telco service" over multiple cloud nodes of the XIFI infrastructure node, and attaching additional technology nodes and components from others private clouds or external single-node platform, e.g. Telecom Italia's one, via XIFI extendible cloud tools.	Developers End Users / Adopters

Table 1: Summary of the selected showcases.

3 SHOWCASES ON XIFI NEW SERVICE DEPLOYMENT

These four showcases have been designed to illustrate the process whereby Technology Providers might benefit from what XIFI has to offer, as well as what Developers can expect when using XIFI facilities. The first looks at a specific application area to illustrate a typical and important service using complementary resource across what the EBM calls "user-centric" and "location-centric" infrastructures. The other three are more practically focused on the logistics of using XIFI to find and access features, as well as to deploy new features that the Developer and/or Technology Provider may have created. This first set, therefore, is about how to use XIFI and what to use it for.

3.1 UC1: E-Health in a Smart City Environment

Partners	DT
Domain	Complex experimental service
Stakeholders	Developers, Technology providers, End Users / Adopters
Relevant XIFI aspects	Demonstration of a service related to smart cities.
Adopted Enablers	S3C GE, Location-LOCS GE, Publish/Subscribe Context Broker - Orion Context Broker GE, WebRTC Handover SE.

Table 2: UC1 Summary table.

3.1.1 Showcase description

3.1.1.1 Motivation

Due to demographic changes the number of elderly people, who want to stay in their home environment as long as possible, is steadily growing. Upcoming smart city technologies could support this goal, but the underlying concepts can be well transferred to other usage scenarios as well. This showcase shows how such a solution can be developed using FI-WARE GEs and deploying new specific enablers on top of XIFI.

3.1.1.2 Target Stakeholders

The target audience are developers and Use Case Projects that wish to use the XIFI environment to build up and test new services. The showcase provides information on how running instances of generic enablers can be used to build a simple use case. Especially the use of 'non-conventional' services like the instance of the mobile/wireless testbed provided in the Berlin node is shown.

3.1.1.3 Scenario

A variety of illnesses exist, where people might experience a sudden health attack, e.g. a vaso-vagal episode. In such a situation the person often requires quick personal assistance, medical service assistance or medical treatment via telecommunication services. In all cases, a medical service button available on the mobile phone – provided as a "hot key" – could be of real benefit. By pressing the medical service button, a video call or in case of bandwidth limitation at least a phone call would be automatically established to a fixed health assistance service or dynamically to the nearest one. Via the video call connection the patient or any nearby person could tell the medical assistant the situation and get quick enhanced treatment. In the case where the situation is already critical, the patient/ calling party could provide any supportive information using the video connection, e.g. show the injury or show the surrounding area to the medical assistance team in addition to the automatically retrieved location information, e.g. inside a building. Therefore the medical assistant would receive supporting information from the video capture. In addition while the medical assistant drives towards the patient,

the call is automatically switched to the device in use (e.g. including handover between different access networks like WiFi LTE/3G). Thus the connection between the medical assistant and the caller is never disconnected while he is moving the incident place.

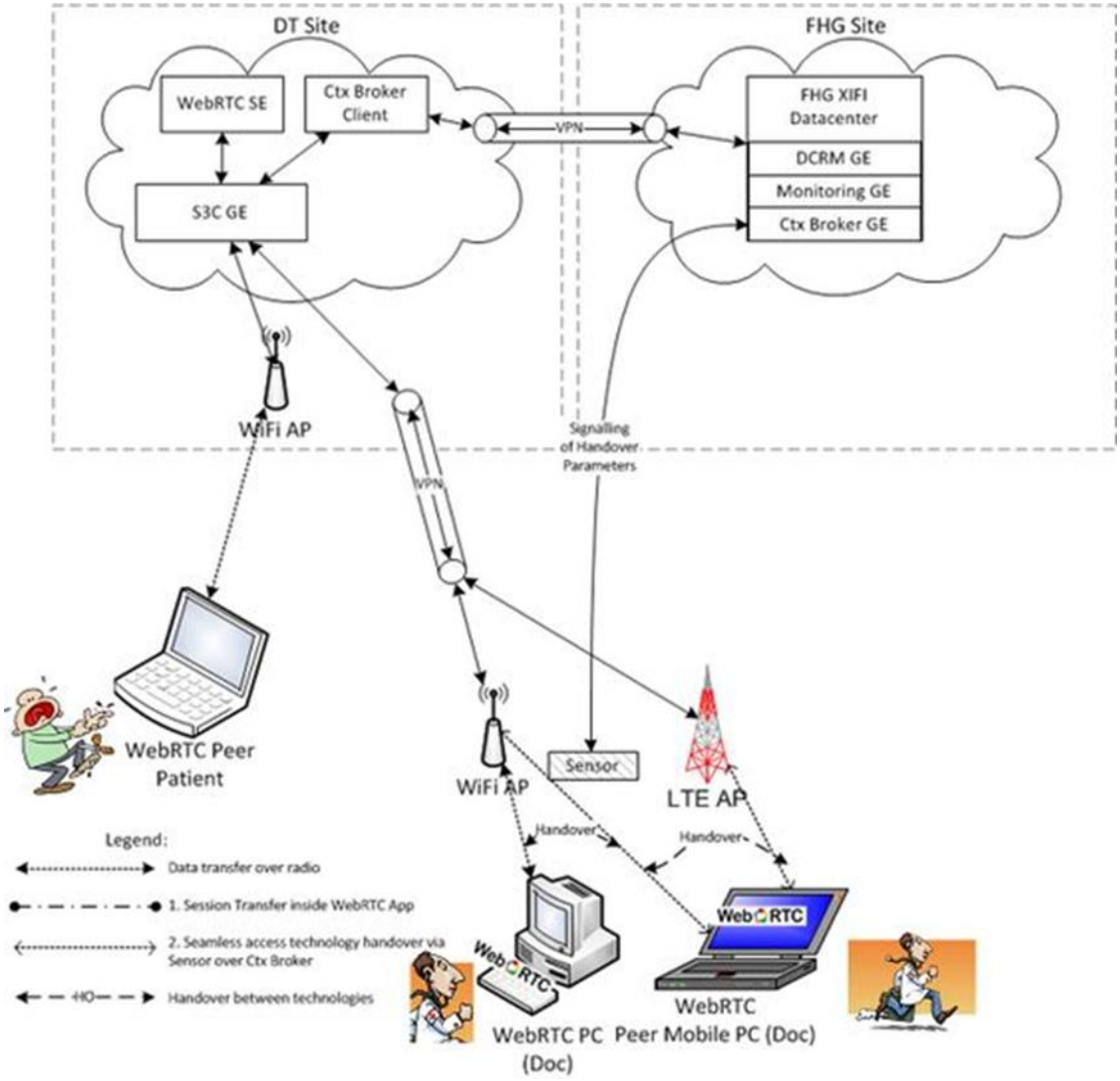

Figure 2:UC1 description.

Actor	Role	Role description	Benefit
Person	Patient	Requires medical assistance away from a medical institution.	Patient does not need to live in a medical institution (hospital). Further, the patient does not necessarily need to stay at home, but can request assistance wherever they undergo an attack.
Medical assistance service	Provides mobile medical assistants	React on emergency call of known / unknown persons	In case of emergency, the medical assistant can help via the voice/ video call connection or is directed to the person requiring help.

Table 3: UC1 actors, roles and benefits summary.

3.1.2 Technical description

This showcase will depict how to deploy a service using the enablers provided by the XIFI federation. The scenario(s) are related to the smart city service domain, particularly to the Smart Living & smart health domain. Depending on the available enablers and sesnors we will demonstrate how to use emergency data in an urban development and to include communication and connectivity services (e.g. WebRTC [1]) as part of the showcase.

The showcase focuses on a mobile scenario and is based on a "medical service button", which could be provided as a "hotkey" on a smart phone. Once the smartphone owner presses the “hot key” automatically the Location information is requested. Initially the location shall be provided via GPS. But in case the GPS signal is missing (e.g. when inside), the location information from the operator network is requested (cellID, tracking area) to locate the user immediately. An important aspect of this showcase is a reliable IP connection using the best available mobile access technologies, e.g. UMTS/LTE or WIFI (provided by the Berlin node). The connection is used for a WebRTC based Video / VoIP IP connection establishment between the patient's mobile device and the pre-installed or (nearest) medical service team with guaranteed service should be possible. As an add-on, the call information could be logged and stored, including a copy of multimedia data generated during the session.

The showcase will show how such a scenario can be built using XIFI nodes providing special purpose environments as provided by the German node. The German node provides a mobile testbed within the premises of DT besides the datacentre provided by Fraunhofer FOKUS. The architecture of the German node is shown in the figure below.

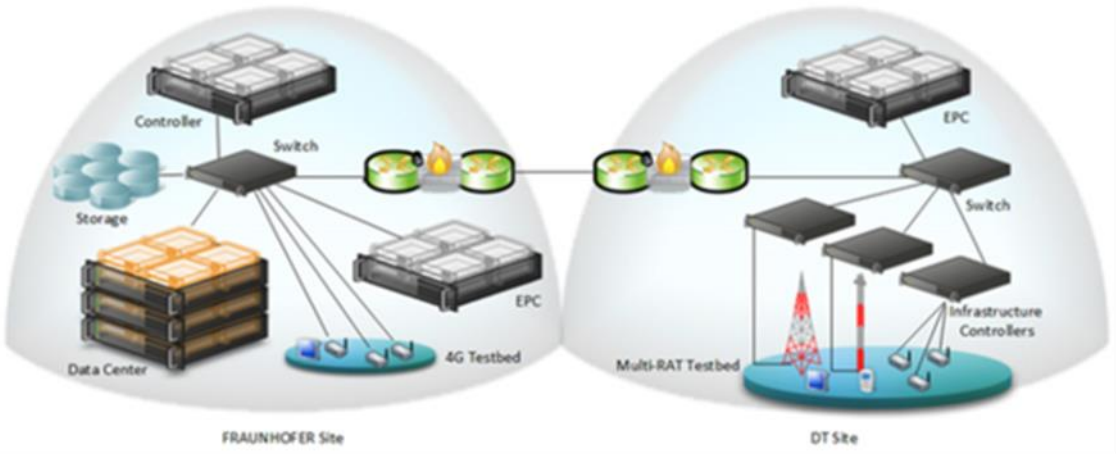

Figure 3: Architecture of the Berlin node.

In particular the showcase will proceed as following:

- Evaluate GEs that could support these services.
- Define the detailed showcase service to be deployed based on available services and resources.
- Develop and deploy showcase.

3.1.2.1 Description of components

Chapter	Name of GE	Short description aligned to use case
Interface to Network and Devices (I2ND)	S3C	This generic enabler will provide the connectivity between the acting parties as well as support the handover between different access

		technologies. The following features will be used that are included in the generic enabler: • Mobility Management, • Connectivity Management, • Network Identity manager It also includes the possibility to allocate different devices to one SIP account.
Data/Context Management	Location - LOCS	This GE may be used to determine the location of the incident site and locate the medical assistant nearest to that site.
Data/Context Management	Publish/Subscribe Context Broker - Orion Context Broker	This GE may be used for providing context related information to trigger a handover to a WebRTC call between different devices and/or access networks.

Table 4: UC1 FI-WARE GEs.

Topic	Name of component	Short description aligned to use case
SE	WebRTC Handover SE	This special enabler will provide the functionality to provide handover between different devices. E.g. the call is handed over from the PC of the medical assistant to the mobile PC (or a tablet) and vice versa.

Table 5: UC1 Self developed parts, SEs.

Other technical aspects: The following figure shows the technical architecture describing the deployment of the needed GEs for the first release of the showcase.

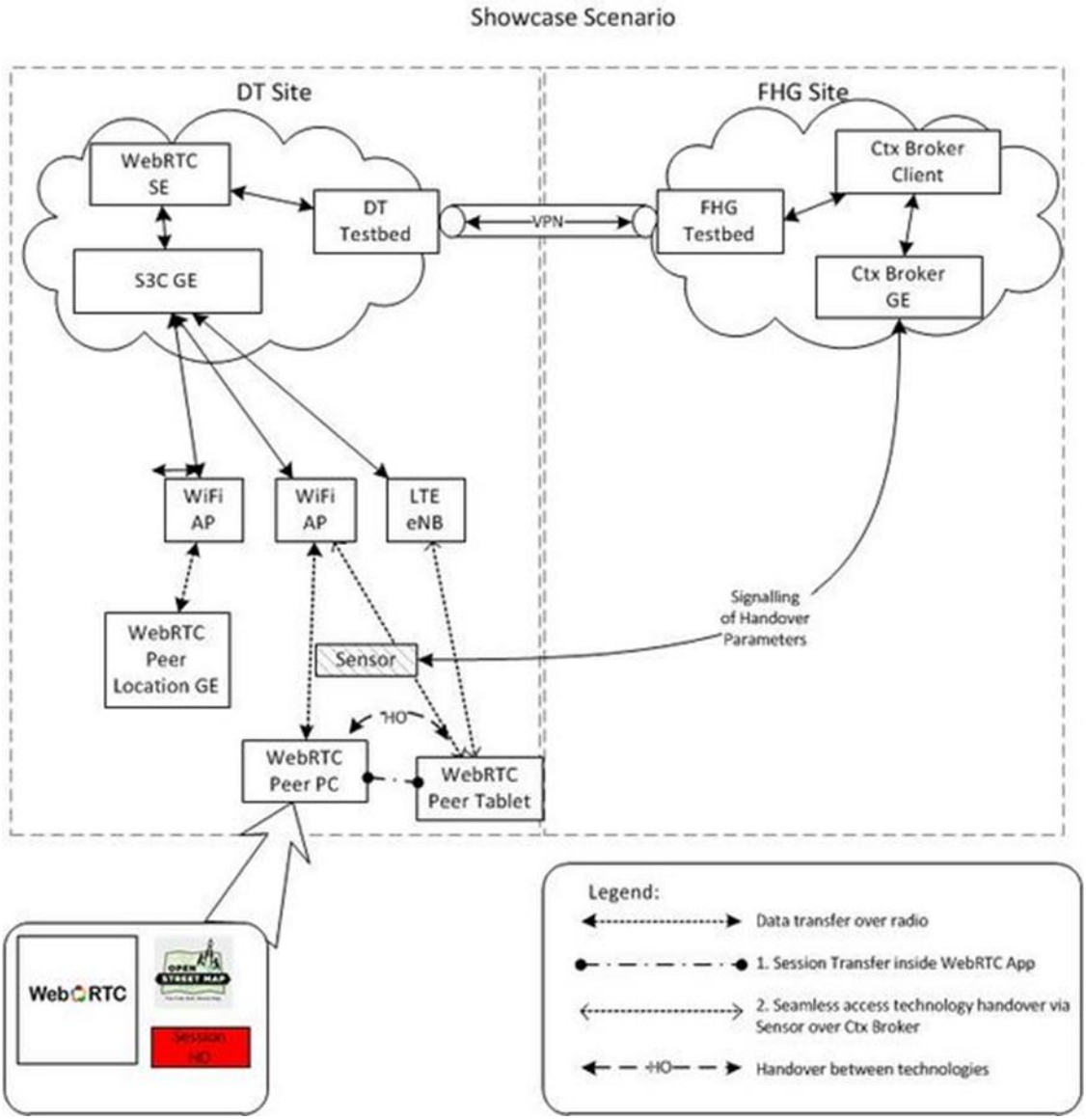

Figure 4: UC1 architecture.

3.1.2.2 Requirements to nodes / other work-packages within XIFI

This use case is using the following enablers:

ORION Context Broker [2]: The Orion context broker will be deployed in the datacentre of the German Node. The client parts will on one hand be on an external device to change the value of a context and on the other hand on the datacentre for triggering a change of the context value to start a handover handled by S3C GE and WebRTC SE. The ORION Context Broker was chosen because of its simplicity. It is easy to handle (to register certain contexts, sent and retrieve information about context values or to subscribe to a context). The lack of security functionalities within the context broker did not matter for the showcase, but should be carefully considered in real world use cases.

S3C GE [3] in a running instance (available at Berlin Node): The S3C GE is used to handover sessions between different access networks using the Mobility Manager feature. The Network Identity Manager feature of S3C will be used to register different end devices of one user to his SIP ID. The S3C GE is deployed in the DT part of the German node. The S3C GE enabler was chosen to show the benefits for Application developers of having knowledge and access to network functionalities. Network functions and information like performance available bandwidth, triggering handovers or choosing the access

network are easily provided to the developer through an interface. The developer can then not only control how the application will behave in a certain access network but also to a certain extent control how the network will behave for a certain application.

Location GE [4]: The Location GE will be deployed on the end device of a user to determine the location of a certain device. The Location GE was chosen to get access to location information of the acting parties within the showcase.

3.1.3 Release plan

1st Release at M12:

First version within a node (Berlin) with the following functionalities:

- Deployment of GE on the Berlin Node
- Deployment of WebRTC SE on Berlin Node
- Registering and publishing.
- Deployment process on the Berlin node of the SE from the XIFI Portal.
- Provide portability of the showcase by connecting Access Points via VPN to the S3C GE instance in Berlin.

2nd Release at M24:

Second version with the same node including:

- Deployment of some GEs needed on another XIFI node (prob. Trento to be discussed)

3.2 UC2: 3-tier GE deployment on multiple sites

Partners	TID
Domain	Inter-Domain connectivity
Stakeholders	Developers, Technology providers, Infras. owners & operators, Public authorities
Relevant XIFI aspects	Dynamic configuration of networks in order to connect servers from different Tiers within the same Blueprint instance.
Adopted Enablers	PaaS Manager, SDC[3].

Table 6: UC2 Summary table.

3.2.1 Showcase description

3.2.1.1 Motivation

There are some cases in which it is necessary to deploy one of the servers from your 3-Tier architecture in one datacentre and another in a separate one. One example is the management of security and regulatory aspects related to personal data, which in many cases cannot go out of the country of the person. Therefore ensuring the reliability of the services/applications deployed in different datacentres configuring the corresponding secure links (using VPN or IPv6 tunnels) is of

[3] SDC (standing for Software Deployment & Configuration) is the usual way this and other deliverables refer to "Software Management & Configuration GE" from the Catalogue.

importance for cloud users and datacentre IT managers.

3.2.1.2 Target stakeholders

Application developers and service providers who must fulfil those special requirements regarding specific location of tiers/components of their services, and need fine-grained control of what, where and how the service gets installed.

3.2.1.3 Scenario

The showcase illustrates how to deploy a typical 3-Tier application using the PaaS Manager in different datacentres and the configuration of the networks between the different servers in order to secure the communications and define a unique way to access to them. This will create a dynamic inter-datacentre network, which allows this secure communication. As the servers are available through the network, these servers can be connected although they are in different datacentres. This means that for this deployment the communication between the different servers will be made only using that predefined secure networks, preventing malicious access or not allow communication or access to data from third parties applications outside the defined service.

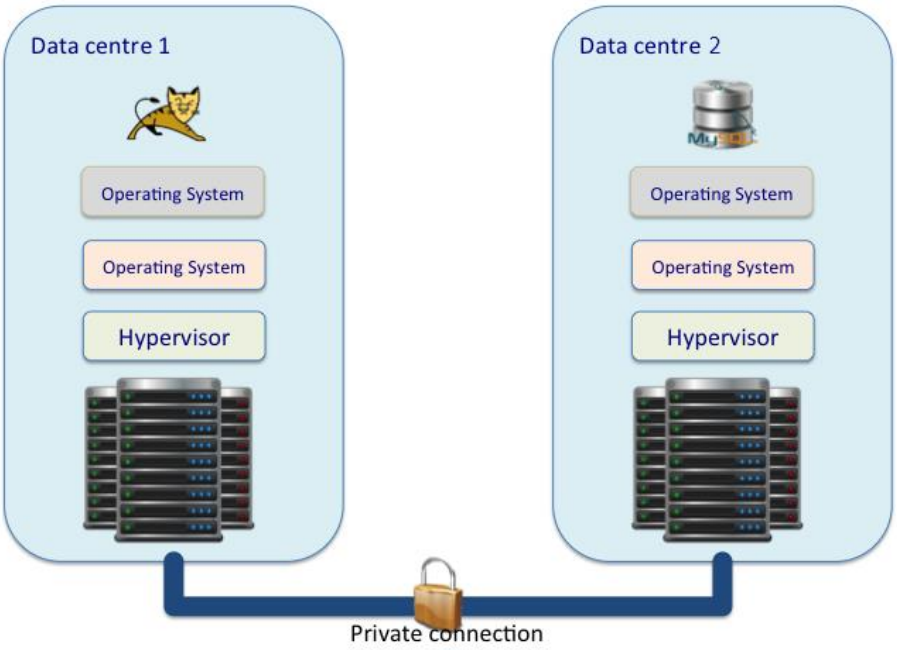

Figure 5: Datacentre interconnection.

3.2.2 Technical description

This showcase will depict the use of a small set of XIFI services related to the configuration of the network (to be identified) to set up a related experiment that illustrates the secure interconnection of servers coming from different datacentres. For this purpose, the functionality of the PaaS Manager to deploy an application/service in different datacentres is used, together with the network enabled GE developed in XIFI can be used to:

1 Deploy a blueprint with 2 or more Tiers on different datacenters (nodes) using the PaaS Manager [5].

2 The definition of the blueprint will include the software to be installed in the different servers

using SDC [6].

3 Provide secure and unique interconnection between the servers in different datacentres.

4 Go into the machine and provide some code examples in order to use the component installed and test that all is working properly.

5 Test that outside of the tiers it is not possible to access those machines using for example SSH or any other tool.

6 Monitor the whole process.

3.2.2.1 Description of components

Chapter	Name of GE	Short description aligned to use case
Cloud Hosting	PaaS Manager	This GE may be used to provide the 3-tier architecture of an application to be deployed in one of several sites.
Cloud Hosting	SDC	This GE may be used to install specific software on each server based on predefined recipes.
Cloud Hosting	IdM	This GE may be used to provide authentication to the overall process.

Table 7: UC2 FI-WARE GEs.

Topic	Name of component	Short description aligned to use case
PaaS connectivity to network plugin	PaaS Manager	This generic enabler should be updated in order to allow the automatic configuration of the network connectivity using the network plugin provided by the XIFI team.

Table 8:UC2 Self developed parts, SEs.

Other technical aspects: N/A.

3.2.2.2 Requirements to nodes / other work-packages within XIFI

Partner involved in this showcase is Telefónica I+D (TID) but including two different teams:

- Network team will provide the components to configure the connectivity between the different datacentres.
- Architectural team will provide the support to the PaaS Manager and SDC [6], and also integration of the PaaS Manager with the network plugin in order to automatically configure this connectivity.

3.2.3 Release plan

1st Release at M12:

First version within a node (TID internal) with the following functionalities:

- Two OpenStack [7] environments (version) with PaaS, SDC, IdM and Cloud Portal installed on them.
- Network Controller plugin installed on the Neutron controller.

- Automatic network definition and VPN configuration between two regions using Neutron API extension.

2nd Release at M24:

Connectivity between Seville and Trento node:

- Seville and Trento configured to be XIFI regions.
- PaaS, SDC, IdM and Cloud portal installed on both environments.
- Network Controller installed on both regions.
- Physical connectivity configured between both regions.
- Automatic network definition and VPN configuration between two regions using Neutron API extension.

3.3 UC3: SE registering and deployment

Partners	ORANGE
Domain	Tools for Infrastructure owners and Service providers
Stakeholders	Technology Providers and infrastructure owners
Relevant XIFI aspects	Specific Enabler registering, Yellow Pages ™, SLA.
Adopted Enablers	Marketplace

Table 9: UC3 Summary table.

3.3.1 Showcase description

3.3.1.1 Motivation

The motivation of the showcase is to demonstrate that infrastructure owners can increase services offered to FI-PPP developers through browsing, SLA negotiation of Specific Enabler targeting a potential business model and PaaS deployment in their node of Specific Enablers.

To this end, it demonstrates the simplicity from a Use Case project point of view to publish a Specific Enabler (including functional and non-functional parameters) in the XIFI portal, and from an infrastructure owner to grasp the added value of existing Specific Enablers published by the XIFI federation.

Moreover, this showcase introduces potential monetization between service providers and infrastructure owners thanks to the access to accounting information.

3.3.1.2 Target stakeholders

The target audience are technology developers that wish to publish a Specific Enabler in the XIFI portal, and infrastructure owners that would like to offer the added value of existing Specific Enablers published by the XIFI federation.

The showcase provides information on how to register and deploy new Specific Enablers. It could also introduce potential monetization between service providers and infrastructure owners.

3.3.1.3 Scenario

This showcase is mainly based on the first functional and technical specifications of the components produced in the framework of WP4 as defined in deliverable D4.1 Service & Tools specification.

Due to this dependency, it will be split into two releases. The first release should focus on a Specific Enabler registration in the XIFI portal and local deployment with the PaaS Manager, registering and instance advertisement on the XIFI portal; whereas the second release should include considering SLA management and usage accounting.

We wish to lay the emphasis on the process that an Infrastructure / Use Case project would need to follow to publish a Specific Enabler than on the choice of the enabler itself. For this reason, we propose to illustrate this showcase with an example of an SE developed by ORANGE. This SE, named KIWANO, is a Scalable Dynamic Spatial Database providing real time location information and communication for moving objects (M2M, Vehicles, drones, smartphones, users, etc.)

For demonstration purposes, this SE will be registered and a trial licence (possibly with limited usage) will be granted to infrastructure owners from the XIFI federation during the XIFI project.

Actor	Role	Role Description	Benefits
Specific Enabler developer	Person in charge of packaging SE for registering in the XIFI portal	Requires virtualization of a Use Case component into a Specific Enable , registering and uploading	To promote software components developed by FI Use Case projects
Federator	Authorize SE publication in the portal Simple validation of the registering request to authorize SE uploading in the portal	To provide control regarding Use Case projects publications	To provide control regarding Use Case project publications
Infrastructure Administrator	Person in charge for instantiation of SE	Installation of SE on local infrastructure and advertisement	Provide new SE offer to local ecosystem

Table 10: UC3 actors, roles and benefits summary.

3.3.2 Technical description

First of all, for the purpose of this showcase based on the example of the ORANGE Scalable Dynamic Spatial Database, we will explain how a UC project could migrate an enabler from a physical infrastructure to the XIFI virtualized infrastructure and to package it in a self-contained Specific Enabler.

Then the UC project is able to start the registration process in the XIFI portal. After having performed the necessary steps for joining the XIFI federation, the showcase will describe the process a Use Case project has to follow with the GUI of the XIFI portal for:

- Defining the SE service offering and non-functional information (infrastructure requirements, deployment and configuration recipes, pricing, license information, etc.) with the Resource repository meta-model description.
- Publishing and uploading the SE in the Repository.

Once the SE is available in the XIFI portal, we will detail (on the basis of the SE chosen for the showcase) the process the infrastructure owner has to follow with the PaaS Manager to deploy the SE on his node.

The second step of the Showcase is to explain how the infrastructure owners can advertise this new resource offering, and propose an SLA to FI-PPP developers. To support this process, we will explore SLA management tools that will we developed by WP4.

Finally, the showcase will explain the process the infrastructure owner and FI-PPP developer need to follow to access accounting information in the XIFI portal regarding usage of this Specific Enabler.

Note: this showcase does not include software development. It will describe a process based on exploration of WP2 to WP4 tools.

3.3.2.1 Description of components

Chapter	Name of GE	Short description aligned to use case
Apps	Marketplace GE (including Registry and Directory, Offering and Demand and Discovery and Matching)	GUI to provide Single Entry Point for the Developers and infrastructure owners
Cloud Hosting	PaaS Manager	To allow Use Case project developers to register and upload SE. To allow infrastructure owners to deploy the SE in the node. To publish new instances.
Security	Identity Manager	Track and trace access to the new SE
Cloud Hosting	Data Center Resource Management (DCRM)	Cloud hosting suite

Table 11: UC3 FI-WARE GEs.

Topic	Name of component	Short description aligned to use case
Resource advertisement	XIFI Resource Catalogue	Infrastructure owners to advertise SE instances
SLA Management	XIFI SLA Manager	To define and manage SLA for the service. SLA accounting.
Geo-localization	KIWANO(ORANGE)	Scalable Dynamic Spatial Database providing real time location information and communication for moving objects (M2M, Vehicles, drones, smartphones, users, etc.). This SE is used for demonstration purposes.

Table 12: UC3 Self developed parts, SEs.

Other technical aspects: One Master node is deployed and offers XIFI federation tools.

3.3.2.2 Requirements to nodes / other work-packages within XIFI

There are clear dependencies with work performed in WP1, WP2, WP3, and mainly WP4.

A XIFI federated infrastructure should be in place, offering services (Portal, SLA management, etc) to interested infrastructure owners.

The Brittany node must be available to deploy the SE.

3.3.3 Release plan

1st Release at M12:

First version within a node (Brittany) with the following functionalities:

- Packaging of the "physical" enabler to a virtualized and self-contained enabler.
- Description of the enabler (functional and non-functional information : pricing model, licence management, etc.) according to the metal model description.
- Registering and publishing the enabler.
- Deployment process on the Brittany node of the SE from the XIFI Portal.

2nd Release at M24:

Second version with the same node including:

- Advertisement the XIFI portal with this new resource (i.e. the instance of SE).
- SLA management and access to accounting information.

3.4 UC4: Marketplace services

Partners	UPM
Domain	Application store
Stakeholders	Developers, Technology providers, Infras. owners & operators
Relevant XIFI aspects	Demonstration of interacting with enablers in the infrastructures through the XIFI Marketplace
Adopted Enablers	Store – WStore GE

Table 13: UC4 Summary table.

3.4.1 Showcase description

3.4.1.1 Motivation

Showcase the marketplace services and use of the enablers in the different infrastructures using the recommendation tool examples.

The objective of the showcase is to present the possibilities of the XIFI marketplace in a single showcase where the developers may play with the enablers with some pre-defined applications and services that the showcase is going to develop which will show some potential uses, more elaborated or complex than the simple use of the marketplace to upload an application to a data centre selected by the user.

3.4.1.2 Target stakeholders

This showcase is intended for application developers who would like to register their application through the marketplace.

3.4.1.3 Scenario

The scenario of the showcase will be the following:

A developer wants to develop an application using some generic enablers; this is the first time using the XIFI marketplace. Rather than being aware of any specific infrastructure s/he wants to have the most powerful resources and bandwidth to keep the application running for a smart city. The enablers which s/he wants to use are not clear, and it is preferable that the resources are selected by the Marketplace and not by the user. Even s/he may be willing to pay a fee if the service is of quality and not very expensive.

After developing with Eclipse™ using the plug-in for the GE the user wants to deploy the service in two different locations and therefore it is possible that the optimal solution is to use two infrastructures. In addition, the user wants to receive information on the performance of the application to debug it and understand if the problem is in the application or in the XIFI infrastructures.

Actor	Role	Role description	Benefit
Developer	App developer using GE and XIFI	Requires app to run in different locations for the best performance	XIFI selects the infrastructures and recommends the way of working
Developer	App developer using GE and XIFI	In addition wants to debug the application and have a better understanding of app execution in RT	XIFI provides a complete performance diagram and data on the app running on the underlying infrastructures.
Infrastructure Owner	Infrastructure owner providing GE over XIFI	Provides app to run in an infrastructure with performance targets	XIFI provides a complete performance diagram and data about monitoring and agreements.

Table 14: UC4 actors, roles and benefits summary.

Figure 6: App developer at the main page of the Maketplace. Available infrastructures are shown and there are also some GE suggestions such as top rated and newest enablers.

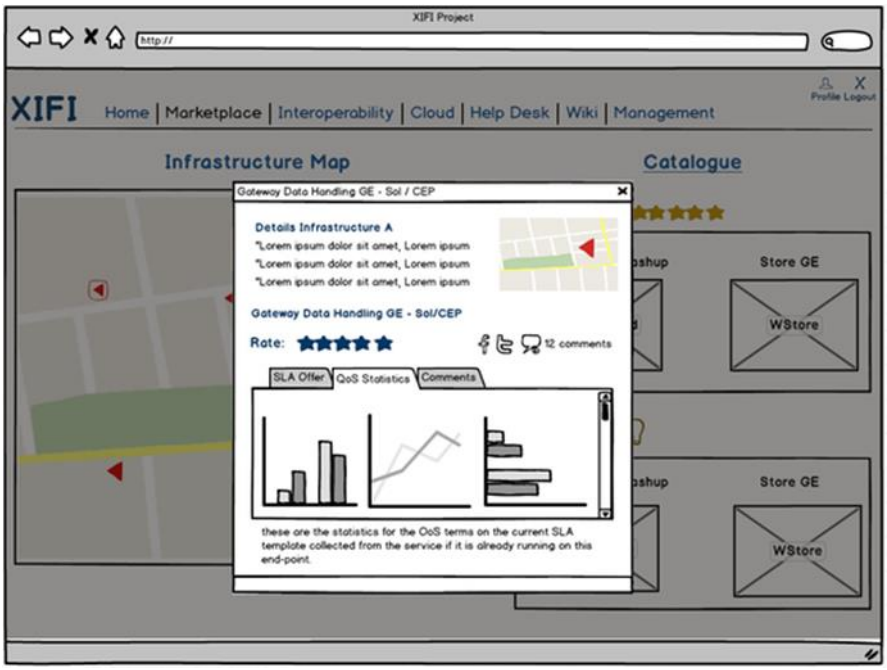

Figure 7: The app developer is also able to gather some detailed information about the different infrastructures.

3.4.2 Technical description

The showcase will explain to the possible XIFI users (mainly developers) the different potentialities of the XIFI marketplace and the selection of the infrastructures useful for their apps.

The service is very close to the way of working of the Marketplace and the recommendation service selecting the best resources and infrastructure depending on the user requirements and profile.

The presentation of the showcase will be mainly visual, and the showcase will step by step show the different identified profiles in XIFI and how the marketplace can easily be used and benefit the XIFI identified users (the showcase will be timely aligned to the marketplace development).

Functionalities of the Marketplace:

1. Searching for offerings and comparing them (Developer)
2. Searching for infrastructures and comparing their performances (Developer)
3. Uploading his/her own application hosted in the recommended/chosen infrastructure (Developer)
4. Registering an infrastructure resource/application (Infrastructure Owner)
5. Viewing resources (Infrastructure Owner)
6. Managing an offering (Infrastructure Owner)

Steps of the showcase:

- App Developer:
  - Logs in the marketplace
  - Gathers dynamic information related to available infrastructures and top rated and newest GEs are suggested
  - Is able to search and compare different GEs through the Resource Catalogue
  - Is supported by the recommendation tool in order to choose the most feasible infrastructure

- Infrastructure owner:
  - Login the marketplace
  - Offers a new GE and deploys it into the infrastructure
  - Sets performance and service agreements

Consequently, this use case is using the Store-Wstore [8], which supports most of these functionalities.

3.4.2.1 Description of components

Chapter	Name of GE	Short description aligned to use case
Applications/Services Ecosystems and Delivery Framework	Store - WStore	Supports both user roles, infrastructure owner and application developer, with their respective actions

Table 15: UC4 FI-WARE GEs.

Topic	Name of component	Short description aligned to use case
Apps	Marketplace	directed implementations of the Marketplace adapted to the user profiles
Monitoring	Test applications	Test applications to show the functionality that will be developed (tailored to the user profiles)

Table 16: UC4 Self developed parts, SEs.

Other technical aspects: Pre-configured case of the Marketplace with additional services and tailored applications with examples

3.4.2.2 Requirements to nodes / other work-packages within XIFI

There is a main and clear dependency with work done in WP4.

The RedIris node should be available.

3.4.3 Release plan

1st Release at M12:

First version within a single node (RedIris).

2nd Release at M24:

Second version across two nodes.

4 SHOWCASES ON XIFI INFRASTRUCTURE PERFORMANCE

A common question that potential users such as developers and SMEs would want to ask is how well an infrastructure or infrastructures might perform in support of their work. This is not simply a question of the capacity and resources available, but also being able to monitor actual performance as well as data management across and between infrastructures. The showcases here target precisely this area, illustrating what needs to be managed and how the federation operates in terms of service quality. The three individual showcases illustrate how to go about monitoring resource performance, as well as the dynamic management of those resources. This includes shaping traffic (bandwidth on demand), configuration management in establishing which resources might be best suited to a task, as well as more traditional performance overviews. Complemented the T6.1 showcases, these are about getting the best out XIFI and the federated infrastructures.

4.1 UC5: Quality of Experience in NaaS

Partners	CREATE-NET
Domain	Video Streaming
Stakeholders	Developers, Technology providers, Infrastructure owners & operators
Relevant XIFI aspects	Network monitoring and dynamic configuration across nodes.
Adopted Enablers	XIFI Network Controller, XIFI Infrastructure Monitoring

Table 17: UC5 Summary table.

4.1.1 Showcase description

4.1.1.1 Motivation

The showcase planned by CREATE-NET will be used to demonstrate how XIFI services related to the network and its dynamic configuration through SDN (Software Defined Networking) technology and NaaS (Network as a Service) facilities at cross-node level. Through network reconfiguration capabilities, the showcase will demonstrate how it is possible to improve QoS perceived by users and/or service reliability.

4.1.1.2 Target stakeholders

The target audience are both developers and users that want to use or explore the XIFI Network functionality. In particular this showcase highlights some features of NaaS in order to improve the QoE of the end-user.

4.1.1.3 Scenario

The emergence of cloud services, including rich-media services, keeps growing in popularity. Examples are distributed computing servers for large data sets and web services. In this context SDN and NaaS are enablers to assure QoS. SDN technology allows network configuration in real time, thereby the efficient use of network resource, while NaaS offers direct tenant access to the network infrastructure and the possibility to adopt application-specific protocols. These allow an efficient deployment of network services. For instance the transfer of big data files between Data Centres (DCs) and Video Streaming applications can be managed with fault prevention to ensure service continuity in case of network failure.

Figure 8: Quality of Experience in NaaS.

Actor	Role	Role description	Benefit
User	User	Requires Video Streaming	User is not aware of the underlying physical network and the architecture, but he can experience a high QoE

Table 18: UC5 actors, roles and benefits summary.

4.1.2 Technical description

This showcase illustrates how to improve QoE using network monitoring and dynamic configuration across nodes. The scenario is related to network control through SDN technology and NaaS facilities at cross node level. The showcase is based on network services and how the user can benefit from the XIFI infrastructure. In the proposed scenario we demonstrate how the user can improve his QoE using a video streaming application. Once the user requests such an application the underlying network is configured in order to ensure service continuity and an appropriate QoS. The XIFI Network Controller is used in order to perform fault prevention or fault recovery in case of network failure. In particular these functionalities:

- PCE (Path Computation Element) [9] to find the primary path (e.g. in terms of delay, jitter, etc.) and a secondary path in case of failure (or degradation).
- NaaS that offers a network abstraction and handles user requests before triggering E2E connectivity

These features are made possible using SDN, NaaS and network monitoring. In particular, to perform fault prevention, it is necessary to use network monitoring. When a degradation of the QoS is revealed, it is possible to set up a new end-to-end connection dynamically by means of SDN features, and then switch from the degraded connection to the new one, which can guarantee a suitable QoS for the user application. Moreover, another possible scenario could be to use a Policy Agent (an advanced functionality of the XIFI Network Controller), giving priority to the video streams that require a certain QoS. This showcase will demonstrate how it is possible, using these features, to improve the Quality of Experience.

The main elements of the showcase are:

- a Media Server (MS) that streams a video to a proxy server
- a Proxy Server (PS) that redirects the video to the user

These elements are hosted in two different VMs. For the sake of simplicity we assume that there is only a PS and that the MS is located in a different XIFI node. Actually there will be more than one PS, and the XIFI Master node could choose the Proxy Server on the basis of geo-location (e.g. a PS in

each XIFI node).

The main steps are the following:

1 The user connects to the XIFI portal

2 Selects to use a Video Streaming service (e.g., an MS located in a node B), requesting a QoS among the MS and the PS (e.g., located in a node A), that is using a NaaS capability (e.g. path protection/restoration) through the XIFI network

3 The NaaS sets up the path(s) by means of the XIFI Network Controller. This path is monitored using the XIFI Infrastructure Monitoring Middleware (XIMM)

4 Once the connectivity is set up, the MS streams the video to the PS

5 The Proxy Server redirects the video to the end-user

6 If the XIMM detects degradation (in case of fault prevention) or a fault in the path across the PS and MS, raise an alarm to the XIFI Network Controller which triggers a new path (restoration) or a pre-configured path (protection)

7 The end user can benefit from a consistent QoE

We assume that NaaS exposes the network functionality which is made possible using the XIFI SDN Controller and XIFI Infrastructure Monitoring Middleware.

4.1.2.1 Description of components

Chapter	Name of GE	Short description aligned to use case
Cloud Hosting	DCRM GE	Provide the computational capacity for the servers used in the showcase

Table 19: UC5 FI-WARE GEs.

Topic	Name of component	Short description aligned to use case
Video	Video Streaming application based on VLC	The video streaming application is deployed on the DCRM GE and its quality of service is monitored by the monitoring adapter.
Software-defined Networks	XIFI Network Controller	The network controller adapts the connectivity according to the quality of connectivity.
Software-defined Networks	XIFI Infrastructure Monitoring Adapter	The monitoring adapter controls the quality of the connectivity.

Table 20: UC5 Self developed parts, SEs.

Other technical aspects: N/A.

4.1.2.2 Requirements to nodes / other work-packages within XIFI

In order to show the XIFI NaaS functionalities, two WP3 components are required: The Network Controller and Infrastructure Monitoring.

XIFI Network Controller (ABNO [10] /OpenNaaS [11])

- Handle user requests (e.g., a request with QoS)
- Calculate a set of paths using PCE (e.g. primary and secondary path)
- Set up/Tear down a path. In particular to perform protection and/or restoration

- (optional) Policy Agent features

XIFI Infrastructure Monitoring

- Detect E2E path degradation/failure
- Trigger the XIFI Network Controller

4.1.3 Release plan

1st Release at M12:

The first version of this showcase will include the installation of the main components, the Proxy Server and the Media Server, in a single node (Trento). Therefore the functionality will be limited to a single domain network.

2nd Release at M24:

Second version across two nodes (Trento and Berlin) with the installation of multiple Proxy and Media Servers. In this release the full NaaS functionalities will be explored in a multi-domain network.

4.2 UC6: SDN traffic engineering

Partners	THALES/HEANET
Domain	Flow management/ Cybersecurity
Stakeholders	Developers, Technology providers, Infrastructure owners & operators
Relevant XIFI aspects	Network monitoring and dynamic configuration across nodes.
Adopted Enablers	NaaS, Bandwidth on Demand (BoD) and Software-Defined Networking (SDN)

Table 21: UC6 Summary table.

4.2.1 Showcase description

4.2.1.1 Motivation

Distributed cloud infrastructures such as XIFI automate the provisioning of compute, network and storage resources so that Internet applications and enterprise systems can operate across several sites with dedicated resources. Such cloud platforms are exposed to great vulnerabilities from intentional threats (cyberattacks, for example) to system failures.

XIFI provides advanced networking capabilities in terms of NaaS, SDN and BoD to interconnect virtual machines inside datacentres (nodes) and between the different sites. The functionalities include connectivity setup, resource allocation (bandwidth on demand), flow monitoring (statistics, DDoS detection) and flow prioritization.

This showcase demonstrates the use of the advanced network monitoring capabilities based on OpenFlow extensions which can be used for traffic engineering and cyber-attack detection.

4.2.1.2 Target stakeholders

This showcase is dedicated to developers that would like to discover the advanced networking functionalities of the NaaS API for traffic engineering.

4.2.1.3 Scenario

The showcase illustrates how an application developer can use the network monitoring services provided by XIFI to increase the QoS and the security of their application. Based on the information reported they can decide to migrate one service from one place to another and request network services thanks to the NaaS APIs:

- request more bandwidth between virtual machines in a datacentre or in-between two datacentres
- specify flow priorities to the network infrastructures.

Actor	Role	Role description	Benefit
Developer and Technology providers	App developer using GE and XIFI	use the network monitoring services provided by XIFI to increase the QoS and the security of their application	Based on the information reported he can take a decision and request network services thanks to the NaaS API

Table 22: UC6 actors, roles and benefits summary.

4.2.2 Technical description

The figure below schematically presents the different levels at which the XIFI network controller manages the different interconnections. The NaaS component receives connectivity requests from the cloud management system and processes them at two granularities:

- Aggregation level: using the BoD (Bandwidth on Demand) services and intra-DC functions to offer aggregated end-to-end connectivity between and inside infrastructure nodes,
- Flow level: using SDN flow management to monitor flow quality, detect abnormal network events, and enforce QoS policies.

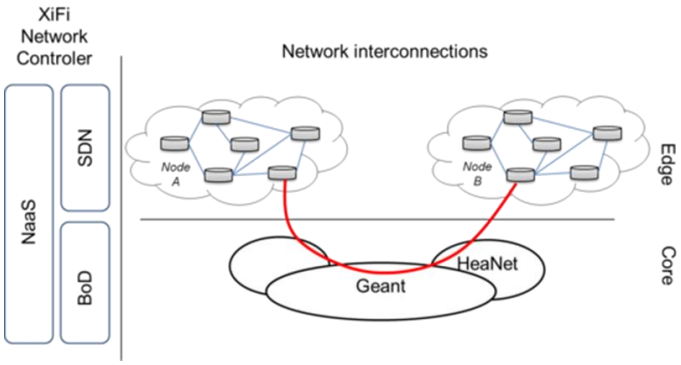

Figure 9: XIFI infrastructure and advanced networking functionalities.

This showcase will depict the use of a small set of XIFI enablers through the following steps:

1. An application developer connects to the XIFI portal
2. Requests N (<10) virtual machines on two different datacentres (XIFI nodes)
3. Asks for network connectivity between the virtual machines with a specific bandwidth requirement for the inter-DC link (e.g. 10Mbits from 1 node to the other)
4. Requests network monitoring for all the intra and inter-DC links (flow statistics)
5. Deploys using SSH test scripts to generate a background traffic scenario
6. Demonstrates the use of BoD services to improve the performances of its application

7. Uploads a set of flow policies using the NaaS API
8. Generates malicious traffic
9. Executes an abnormal event attack identification (e.g., DDoS) task using the Big data analytics GE (analysis of port/source entropy)
10. Monitors the whole process using the different monitoring and security dashboard.

4.2.2.1 Description of components

Chapter	Name of GE	Short description aligned to use case
N/A	N/A	N/A

Table 23: UC6 FI-WARE GEs.

Topic	Name of component	Short description aligned to use case
Software-defined networks	XIFI Network Controller	To adapt the network connectivity
Monitoring	XIFI Infrastructure Monitoring Adapter	To monitor the status of the network connectivity

Table 24: UC6 Self developed parts, SEs.

Other technical aspects: N/A.

4.2.2.2 Requirements to nodes / other work-packages within XIFI

Functional requirements for XIFI network components:

- Network as a Service (NaaS)
  - Request a given network connectivity between end-points
    - 10Mbits/s between nodes A and B
    - 100Mbits/s between VMs inside a node
  - Upload flow priorities
- XIFI Infrastructure Monitoring
  - Retrieve flow statistics
  - Analyse abnormal events (e.g., DDoS)

Behind the NaaS service, the Bandwidth on Demand (BoD) and Software-Defined Networking (SDN) components should take care of setting up the network connectivity, applying QoS policies, updating bandwidth allocations and monitoring intra-DC and inter-DC links.

Hardware and software requirements :

- 10 virtual machines on 2 XIFI Nodes (to be defined depending on BoD capabilities)
  - GB of RAM, 1 CPU core and 4GB of hard-disk each
  - Ubuntu

4.2.3 Release plan

1st Release at M12:

The first version will be without BoD and will demonstrate only the monitoring part.

2nd Release at M24:

Second version with BoD and will demonstrate the application of developer policies (e.g., priorities).

4.3 UC7: Monitoring QoS in the Node

Partners	TN
Domain	QoS
Stakeholders	Developers, Infrastructure owners & operators
Relevant XIFI aspects	Network and QoS monitoring inside nodes.
Adopted Enablers	Context Broker GE, Network Adapter Module (NAM).

Table 25: UC7 Summary table.

4.3.1 Showcase description

4.3.1.1 Motivation

XIFI users may need to evaluate the node situation in terms of availability, network connectivity between other nodes, and free internal resources to correctly deploy GEs. The aim of the showcase is to show how, analysing certain QoS parameters offered by monitoring tools, it might then be possible to evaluate the status of a node and its suitability for deployment of one GE or another in order to deploy everything in the best way using the most appropriate node for every application. Note: this showcase differs from the previous one (Section 4.2) which has more of a traffic management bias than specific node performance.

4.3.1.2 Scenario

The user will be free to deploy a GE on any node, but not all the nodes are identical and due to such differences an application might be able to find a more suitable infrastructure to run that particular GE and that particular time. It's important for the user to be aware of all the requirements of the desired application, and also the QoS availability of each node, in order to match the best deployment solution. This showcase will show the possibility of monitoring some critical parameters on the hardware and software running in the node, to give to the users the opportunity to evaluate the QoS on the node and select the correct node where deploying a given GE would maximize the efficiency of any associated experimentation.

Actor	Role	Role Description	Benefits
Developer	Who develope applications, using GEs	check for the local resource and connectivity performance	Ensure the selected node meets the user requirements for the specific application
Infrastructure Owner	Technicians who mantain DC and GE instantiations	check for the local resource and connectivity performance	Monitoring operation and resourse check to evaluate the performance on the single node and between pairs

Table 26: UC7 actors, roles and benefits summary.

4.3.2 Technical description

Using the XIFI adapters that collect information provided by passive monitoring tools, already running on the infrastructure it will be possible to know, at a glance, the situation inside each node in terms of:

- CPU Usage
- HDD Space Usage
- Memory RAM Usage
- Temperature CPU
- System Uptime
- # Processes running
- # Users
- Status of Processes

In term of active monitoring, using the NAM adapter [12], it will be possible to actively test the interconnection between two different servers (hosts) inside the same site testing to check intra-node connectivity, or between servers running in different sites testing, in that way, the inter-node connectivity.

A Graphical User Interface (GUI) could be used to display to the users all the data in different ways, like for example as showed in the following picture.

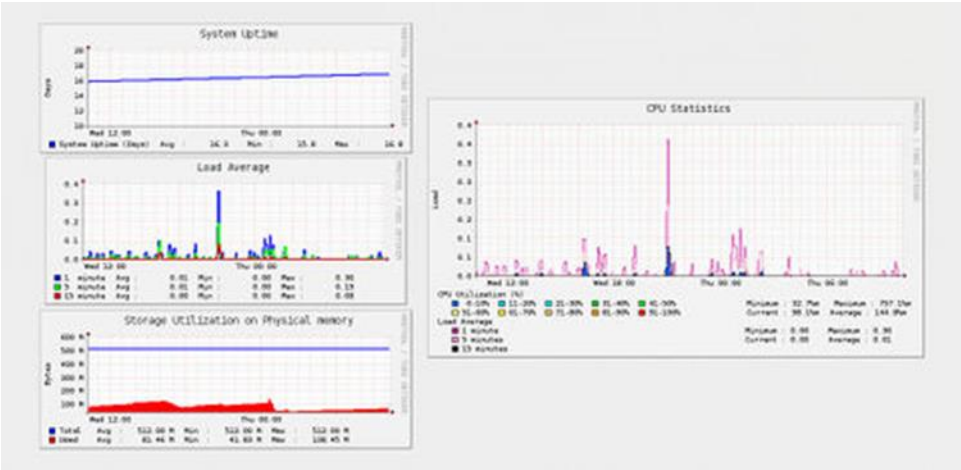

Figure 10: Statistics example.

The main steps are the following:

1. the user will define the requirements for their application, and then connect to the XIFI portal
2. the user could select a node (or more) where the application should be deployed choosing from all the available and check for the local resource and connectivity performance.
3. If the selected node meets the user requirements then the assessment ends. If not, the user will be informed about the lack of compatibility and could then choose another node for the resource check.

The process ends with the identification of one or more nodes which meet the user requirements.

4.3.2.1 Description of components

Chapter	Name of GE	Short description aligned to use case
Data/Context Management	ORION Context Broker	Context Broker GE, to collect and publish information provided by every monitoring system platform.

Table 27: UC7 FI-WARE GEs.

Topic	Name of component	Short description aligned to use case
Monitoring	NMS adapters	Network Monitoring System already running in the node (eg: Nagios, OpenNMS, Zabbix ecc...), for the passive monitoring of the resources, with specific adapters and or plugin to collect the data developed in WP3.
Monitoring	NAM	Network Adapter Module (NAM) for the active monitoring and connectivity performance evaluation [12].
Monitoring	XIFI Infrastructure Monitoring Middleware	The XIFI Infrastructure Monitoring Middleware (XIMM) aims to offer unified control and access to performance metrics coming from different nodes belonging to the XIFI federation.

Table 28:UC7 Self developed parts, SEs.

Other technical aspects: N/A.

4.3.2.2 Requirements to nodes / other work-packages within XIFI

This showcase uses the deliverables produced by within XIFI WP2, WP3, and WP4, and need:

- availability and reachability of the nodes with an OpenStack up and running installation.
- installation of the XIFI adapters on the nodes to enable the monitoring services.

4.3.3 Release plan

1st Release at M12:

Within this showcase, OpenStack and XIFI related services, GEs and monitoring adapters will be installed on the node. First version within a single node (Trento) will provide the monitoring inside a single node referring to the local resources.

2nd Release at M24:

The second version will cover more nodes and in particular will be improved with the inter-node resource check.

5 SHOWCASES ON THE BENEFITS FOR XIFI INFRASTRUCTURES

One of the main objectives of XIFI is to provide the capacity required by the FI-PPP, and this can only be done through the federation of appropriate resource to be accessible to Technology Providers and Developers in support of their development activities. Manuals and guidelines for a node joining the federation may not provide real experience nor the appropriate level of motivation. The showcases here therefore seek to provide practical illustrations of how a new infrastructure might join, identifying any specific areas which need specific attention along the way, but also why the infrastructure should join by showing the services and capabilities which come with federation membership in support of that infrastructure's activities. In T6.1 and T6.2, the showcases focused on what is already available and how best to use it. These showcases, by contrast, are about what needs to be done when new infrastructures want to join the federation for the benefits it offers.

5.1 UC8: Join the XIFI federation

Partners	CREATE-NET
Domain	Infrastructure Toolbox
Stakeholders	Infrastructure owners & operators
Relevant XIFI aspects	Demonstration of how add a new node to the XIFI federation
Adopted Enablers	DCRM GE

Table 29: UC8 Summary table.

5.1.1 Showcase description

5.1.1.1 Motivation

This showcase will be used to demonstrate how to add a new node to the XIFI federation. The deployment and configuration of a new node, where each one is composed of several servers, as well as their connection to the federation, is a complex task for an Infrastructure Owner. Furthermore, it is also very important to organize and ensure a systematic maintenance process.

The process will be supported by a tool named Infrastructure Toolbox, which provides a ready-to-use server starting from a bare metal server. Every server should have the operating system, the hypervisor and the cloud management software. Furthermore, they should be ready to connect to the federation.

5.1.1.2 Target stakeholders

The main target audience is Infrastructure owners.

5.1.1.3 Scenario

The showcase illustrates how an Infrastructure Owner is supported in the addition and testing process of a new node into federation.

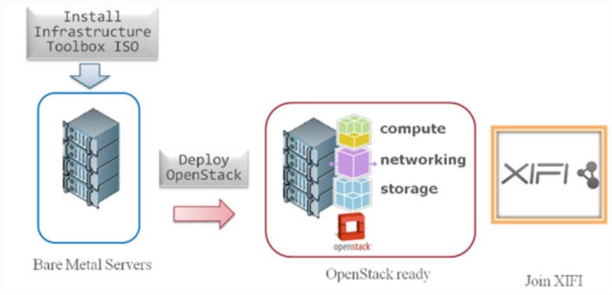

Figure 11: ITBox Deployment Schema.

We will proceed as follows:

- Installation of the Infrastructure Toolbox on a management server, named ITBox server.
- Provision of several servers with the host operating system, hypervisor and cloud software through the Preboot eXecution Environment (PXE).
- Selecting a deployment model (simple cluster, High Availability).
- Assigning of a role to each server: controller, compute, storage, monitoring.
- Installation and configuration of the required software, based on server role.
- Reporting to Federator the results of the deployment and federation test.

Actor	Role	Role description	Benefit
Infrastructure Owner	The main reference of a XIFI node	He manages and deploys services on a XIFI node.	ITBox ensures that the connection of a node to the federation, the maintenance and the up-date process are simplified as much as possible.
Federator	The main reference of the XIFI Federation	He manages and monitors the XIFI Federation	The systematic and supported deployment process helps the Federator to manage and to monitor efficiently the Federation.

Table 30: UC8 actors, roles and benefits summary.

5.1.2 Technical description

The Infrastructure Toolbox (ITBox) is a modular tool, composed mainly of a user interface and a middleware layer. The user interface, named ITBox Interface, provides the Infrastructure Owner with a web based interface for the main functionalities and a command line interface for advanced functionalities. The middleware, named ITBox Middleware, provides the services for the provision and deployment of OpenStack [7] modules and GEs on servers. In detail, the ITBox Middleware is composed by:

- the Host OS Provisioner that installs via PXE the operating system chosen from an operating system catalogue
- the Software Deployment and Configuration (SDC) is a server that provides all necessary packages
- the Orchestrator which coordinates all deployment and installation processes.

ITBox is distributed as an ISO image, which contains an installer for ITBox Master Server. The ISO image can be installed in different ways, using VirtualBox or another bare-metal server. Once installed, ITBox can be used to deploy and manage OpenStack clusters. It will assign IP addresses to the discovered server, perform PXE boot and initial configuration, and provide OpenStack nodes

according to their roles in the cluster. Obviously, the ITBox Master Server and other servers must be on the same network. Once the Master server is installed, all other servers can be powered on and the Infrastructure Owner can log in to the ITBox UI, or can start using the command line interface. The cluster's servers will be booted in bootstrap mode (CentOS based Linux in memory) via PXE and thus these servers will be seen by the system as "discovered". At this point the Infrastructure Owner can create an environment, add servers to it, and start configuration. In more detail, the steps to run are:

- On each server, the Infrastructure Owner selects PXE boot and enables the CPU Virtualization.
- The Infrastructure Owner boots the servers in boostrap mode. When, the boostrap is installed, the servers are in "discovered" state, and they are usable by ITBox.
- Creation of a new environment (also named project). The Infrastructure Owner can select installation options: operating system (Ubuntu 12. 04), hypervisor (KVM), network plugin (Neutron), Cinder, Glance and DCRM GE [13].
- The Infrastructure Owner assigns a role to every server: Controller, Compute, Block storage.
- Verification of cluster network settings. Thus, the Infrastructure Owner can test if the cluster is well configured.
- After all the previous steps are accomplished, the Infrastructure Owner can finally trigger deployment on servers.
- When the deployment process is finished, the Infrastructure Owner runs a test in order to verify the correct installation of all cloud environment modules and if the node is ready to join the federation.

5.1.2.1 Description of components

Chapter	Name of GE	Short description aligned to use case
Cloud hosting	IaaS Data Center Resource Management	Installation of the Data Center Resource Management

Table 31: UC8 FI-WARE GEs.

Topic	Name of component	Short description aligned to use case
Video	Video clip	We will provide a video which shows the installation steps of a new XIFI node.

Table 32: UC8 Self developed parts, SEs.

Other technical aspects: N/A.

5.1.3 Release plan

1st Release at M12:

The first release of this showcase will include the installation of Ubuntu 12.04 LTS, deployment and provisioning of OpenStack components (Controller, Compute, Storage), starting from bare-metal servers.

2nd Release at M24:

The second release will include the installation of the DCRM GE, the IdM GE, the Monitoring GE and it will test if the node has been correctly installed and is ready to join the federation.

5.2 UC9: Federated Login

Partners	ENG
Domain	Identity Management
Stakeholders	Developers, Infrastructure owners & operators
Relevant XIFI aspects	How to implement a federated login on a trusted IdM external to XIFI.
Adopted Enablers	Identity Management GE – KeyRock GEi

Table 33: UC9 Summary table.

5.2.1 Showcase description

5.2.1.1 Motivation

Some of the most common issues to deal with in any kind of application are related to:

- Access;
- Authentication;
- Authorization.

This Showcase considers the usefulness for users of a trusted company for accessing the XIFI services by authenticating themselves on an external Identity Manager (belonging to another IdM domain). In the proposed Showcase this is achieved by adopting SAML [14]. SAML (Security Assertion Markup Language) is a protocol for federated login, which means that a user can log in to a given (preferred) IdM and, then, access protected resources/services/application under the control of another trusted IdM.

5.2.1.2 Target stakeholders

Any developers wanting to access the protected services and resources hosted by or accessible through the XIFI Portal and/or the applications and GEs that belong to the XIFI Domain.

5.2.1.3 Scenario

Actor	Role	Role description	Benefit
XIFI developer	Service/Resource Requester	Request to access the XIFI protected services and/or resources	The developer does not need a XIFI registration, needs only to have a profile on a trusted IdM.
XIFI Portal	Portal	Interface for the developer, hosting services/links to services	Supporting a further protocol (SAML) will represent for the XIFI Portal an added value in terms of usability.
XIFI IdM	Identity Management System of XIFI	Storage and management of registered XIFI developer profile information and credentials. Provision of the SSO login mechanism	It allows the XIFI Portal to accept a user (developer) authenticated on external trusted IdMs
Trusted	Identity	Identity Management	The developer already registered to the

External IdM	Management System of a trusted Company	System or Provider from a different Domain, which is trusted by XIFI that stores and manages the profile information of the developer.	IdM System of a trusted Company from a different Domain, can access XIFI services, resources, applications.

Table 34: UC9 actors, roles and benefits summary.

The following figure "Ask for Service" Use Case depicts the "Ask for Service" Use Case. It is extended with "External Login", "XIFI User Registration" and "XIFI Login" Use Cases.

Even though this Showcase only involves the "Ask for Service" UC (extended with "External Login" UC), in order to have a comprehensive overview, all the possible <<extend>> UCs are also reported.

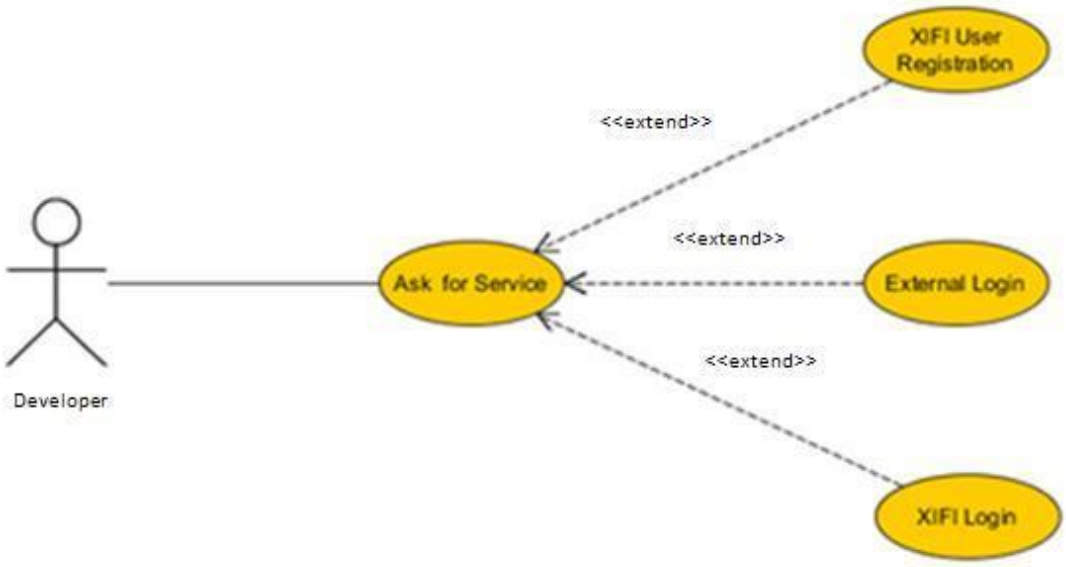

Figure 12: "Ask for Service" Use Case.

1. The developer requires a protected service (or resource)

2. The XIFI Portal asks the developer to log in to XIFI or into another Domain, or to register him/herself on the XIFI Portal

3. The developer makes a choice

4. <<extend>> "Registration" UC (this UC is not yet defined, since it's not in the scope of this Showcase, that considers any user already registered into XFI Portal or any other Domain)

5. <<extend>> "XIFI Login" UC

The developer inserts Username and Password

The developer confirms data inserted by using the "Enter" key or "Sign in" button

6. <<extend>> "External Login" UC

XIFI IdM redirects the developer to the IdM of the selected trusted external Company

The developer logs in using the specific mechanism required by the IdM of the selected trusted external Company

The external Company IdM redirects the developer back to the XIFI Portal/Service

7. XIFI IdM updates and sets the developer's state to the “logged in” state

8. The developer accesses protected and requested service/resource

The “XIFI Login” and the “External Login” UCs are mutually exclusive: this means that the developer doesn't need to log in twice for a single session.

- All the possible sequences are detailed below:
- The developer that has a XIFI registration will follow steps 1,2,3,5,7,8.
- The developer that wants to use an external authentication will follow steps 1,2,3,6,7,8.
- The developer that is not registered to XIFI IdM and that cannot or does not want to access using an external login (or that wants to be registered on the XIFI Domain) will follow steps 1,2,3,4.

The next figure is a sketch of what will be shown to the developer who requests access to a protected resource or service, in the case where that developer is not logged in to XIFI.

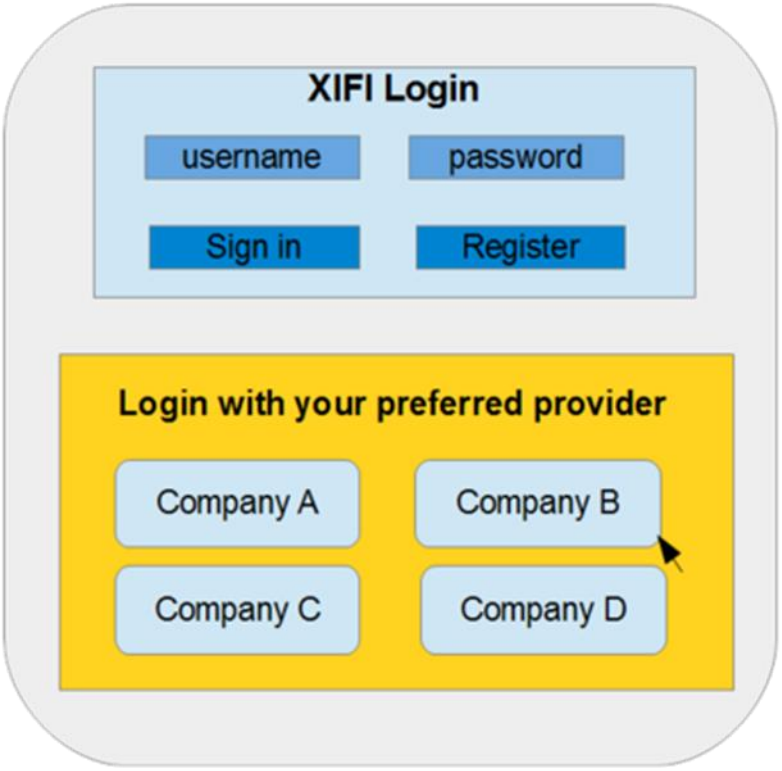

Figure 13: XIFI Login.

5.2.2 Technical description

The scenario represents the case of an application developer of a given Company that asks for a XIFI protected service or resource. The system allows such a user to log in to the IdM (Identity Manager) of the given Company and then allows the developer to access the requested service.

The FI-WARE Identity Management - KeyRock [15] already supports the Single Sign On for local login. Once SAML will be integrated into the XIFI IdM, the external login, i.e. the login that takes place on an IdM external to XIFI, will be handled as local login, and allowed also for Single Sign On in the XIFI Portal. This means that the developer is logged in not only for the requested service(s), but

also for all the other services hosted by XIFI Portal for which he/she has authorization. Depending on internal XIFI rules, such authorization could be static or inferred just in time, as a result of a previous process. This process follows the SAML protocol specification, and for this reason both parties – the XIFI IdM and the external IdM - have to understand SAML assertions. A solution for the integration of SAML in the IdM GE will be provided in the deliverable D2.2, Identity Management [16].

5.2.2.1 Description of components

Chapter	Name of GE	Short description aligned to use case
Security	KeyRock IdM GEi	This stores profile information and credentials of registered XIFI users.

Table 35: UC9 FI-WARE GEs.

Topic	Name of component	Short description aligned to use case
Identity Management	XIFI Federated IdM	The XIFI Federated IdM support SAML 2.0 Profile for Service Provider and Identity Provider and it's used to integrate in the federation other IdM solutions
Identity Management	Third party IdM with SAML support	A third party IdM is connected to XIFI Federated IdM through SAML 2.0 Protocol.

Table 36: UC9 Self developed parts, SEs.

Other technical aspects: N/A.

5.2.2.2 Requirements to nodes / other work-packages within XIFI

This Showcase requires a XIFI Federated IdM installed and available (on a XIFI node) and another external IdM, trusted by XIFI Federated IdM, available too.

5.2.3 Release plan

1st Release at M18:

Deploy the XIFI Federated IdM in ENG test node and connect it to a third party IdM to show how Identity Federation can work through SAML in XIFI Federation.

5.3 UC10: Security monitoring

Partners	THALES/ATOS
Domain	Security
Stakeholders	Infrastructure owners & operators
Relevant XIFI aspects	Demonstration of the XIFI federation resource security monitoring.
Adopted Enablers	Security Monitoring GE, others (to be evaluated).

Table 37: UC10 Summary table.

5.3.1 Showcase description

5.3.1.1 Motivation

The XIFI Security and Privacy Dashboard, integrated into the XIFI Marketplace Portal, will provide information on the security alarms of the different resources provided by the Infrastructure Owners and if those resources fulfil the privacy requirements.

The security monitoring will allow to monitor the federation resources against security risks, collecting events from security probes installed on each node and providing the ability to consolidate, correlate them in advance and make use of attack path computation to direct the work of the Infrastructure Owners and Federator while anticipating the evolution of the attack, and thereby to engage appropriate countermeasures. The Security and Privacy dashboard will be used to visualize alarms and generated reports.

5.3.1.2 Target stakeholders

The main target audience are the XIFI Platform administrators but also the Infrastructure Owner system administrators who can use the Security Dashboard to visualize events and security incidents generated in their nodes.

5.3.1.3 Scenario

The XIFI infrastructures and Future Internet services can be exposed to different types of threats that can lead to severe misuse and damage. This is even more important in a dynamic environment with distributed nodes and services where new threats and attacks can emerge daily.

In this context, the Security Monitoring GE [17] offers an efficient way to detect and respond quickly to security incidents. The use of a Security Dashboard integrated with the Marketplace Portal is essential so that the user can have a tool to easily visualize and check the security risks and react in consequence.

Actor	Role	Role description	Benefit
Person	Attacker	Tries to compromise or gain access to a node in the federation	Attacks are quickly detected.
Person	Federator / Infrastructure Owner	Evaluate level of risk based on alarms received, trigger actions and evaluate their impact	In case of an attack, the Federator or the Infrastructure Owner can visualize an alarm via the Security Dashboard and identify its origin, estimate its target and its propagation, and generate reports so he/she can apply countermeasures to avoid it.

Table 38: UC10 actors, roles and benefits summary.

5.3.2 Technical description

This showcase will depict how to monitor security events generated by the XIFI federation to detect security risks and visualize generated alarms and reports. The scenario(s) where this showcase will focus is still under analysis. Some examples could be: detection of attacks by login brute force, network flow analysis, man in the middle, data extraction, access violations.

We will proceed as follows:

- Identification of requirements to install security probes in each slave node to collect security events (e.g. IDS, firewalls, ...).
- Identification of requirements and definition of API to integrate the XIFI Security Dashboard with the Security Monitoring GE.
- Definition of the security risks to be detected.
- Definition of advanced correlation rules to generate rich (documented) alarms exploitable by an Attack path engine.
- Demonstrate the use of XIFI tools fully exploiting the Security Monitoring GE from FI-WARE to monitor security risks in the Federation and support Infrastructure Owners and Federator in the decision-making process.
- Demonstrate how to configure and use the Security & Privacy Dashboard fully exploiting Security Monitoring GE features to visualize alarms and security events.

5.3.2.1 Description of components

Chapter	Name of GE	Short description aligned to use case
Security	Security Monitoring	This generic enabler offers all the features required to enable the targeted scenario (Service Level SIEM, MulVAL Attack Paths Engine, Scored Attacks Paths, Remediation).

Table 39: UC10 FI-WARE GEs.

Topic	Name of component	Short description aligned to use case
Security	XIFI Security and Privacy Dashboard	This Dashboard is integrated in the XIFI Marketplace Portal. To be defined after evaluation (Task 4.5).

Table 40: UC10 Self developed parts, SEs.

Other technical aspects: N/A.

5.3.2.2 Requirements to nodes / other work-packages within XIFI

Availability of WP4 tools (Security & Privacy Dashboard).

5.3.3 Release plan

1st Release at M12:

The first version will probe the possibility of running the XIFI Security Dashboard to monitor a node against security risks. The functionalities included in this first release will be:

- Installation of Security Probes in a slave node (e.g. Trento node)
- Installation of the Security Monitoring GE and Security Dashboard in the master node (e.g. RedIRIS node)
- Configuration of the Security Monitoring GE to detect some common security incidents in the slave node.
- Visualization through the Security Dashboard of the security alarms and events detected and generation of a simple summary security report in PDF.

- Visualization of accountability events received from the Access Control GE installed in the slave node.

2nd Release at M24:

The second version will probe the possibility of running the Security Dashboard integrated into the XIFI Marketplace Portal by the Federation Security Officer to monitor accountability events generated by the federation resources. The functionalities included in the second release will be:

- Configuration of the Security Monitoring GE to detect security incidents with accountability events received from different slave nodes.
- Configuration of accountability visualization needs in the statistic tool included in the Security Dashboard.
- Visualization through the Security Dashboard of accountability security incidents detected and statistic information.
- Generation of security accountability reports.

5.4 UC11: GE monitoring

Partners	SYNELIXIS
Domain	Infrastructure Monitoring
Stakeholders	Developers, Infrastructure owners & operators
Relevant XIFI aspects	Datacentre and Generic Enablers (DEM) monitoring adapter.
Adopted Enablers	Monitoring GE - TID Implementation, Publish/Subscribe Context Broker – Orion Context Broker, DEM monitoring adapter.

Table 41: UC11 Summary table.

5.4.1 Showcase description

5.4.1.1 Motivation

The main motivation of this showcase is to demonstrate the simplicity from an Infrastructure Owner point of view to grasp the added value of the XIFI federation, through the deployment of datacentre and Generic Enablers monitoring adapters, offering opportunities to support new business models, by collecting and linking monitoring data from GEs deployed in the federation. Moreover, DEM adapter [18] monitoring data will become available to third-party developers and experimenters. The deployment of the DEM adapter is mandatory for an Infrastructure Owner, as part of becoming a member of the XIFI federation.

5.4.1.2 Target stakeholders

The target audience are developers and Infrastructure owners and operators that will be given the opportunity to gather, display and track performance of deployed GEs in the XIFI federated nodes. This showcase provides information on the easy process to set up the monitoring environment and gather monitoring data.

5.4.1.3 Scenario

The core concept of this showcase is to demonstrate the benefits arising from the deployment of the DEM monitoring adapter both from the standpoint of an Infrastructure Owner, as well as for an stakeholder or application developer.

For an Infrastructure Owner, monitoring targeted data on the physical or virtual servers will reveal either a malfunction of a running process/application or a security threat.

On the other hand, gathering of monitoring data offers the possibility to the application developer to check the signed SLA and act accordingly.

Actor	Role	Role Description	Benefits
Infrastructure Owner	Person in charge of monitoring DC and GE instantiations	Requires monitoring of specific data on the physical and/or virtual servers through an easy to use tool	The simple process of deployment of the XIFI DC and GE monitoring adapter will allow for monitoring and gathering data, both on node and federation level
Application Developer	Entity providing a specific application, using GEs	Requires monitoring data for verifying the signed SLA	The monitoring adapter developed within XIFI will offer this capability

Table 42: UC11 actors, roles and benefits summary.

5.4.2 Technical description

The starting point of this scenario is when the infrastructure owner has performed the necessary preparatory steps including the verifications (in terms of compatibility and necessary resources) to become a member of the XIFI federation. In other words, the necessary Cloud Hosting GEs have been installed on the infrastructure.

Within this showcase, the DEM monitoring adapter will be installed on the infrastructure (physical server) and the VMs hosting the GEs, in order to monitor data related to the operational characteristics of the DC and the GEs.

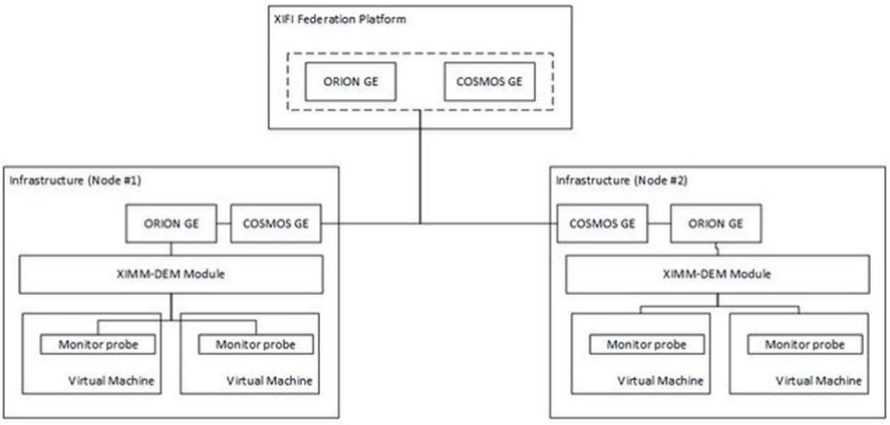

Figure 14: Overview of monitoring architecture in XIFI federation.

Then, the ability to collect (subscriptions through the Publish/Subscribe Context Broker – Orion Context Broker [2]) monitoring data, either at the node level or the federation level, will be demonstrated. In detail, this showcase consists of the following steps:

(Note: Steps 1-5 are part of the first release of this showcase, while step 6 belongs to the second release)

1. Install the DEM adapter on the physical node of the Infrastructure Owner.
2. Through an instance of Publish/Subscribe Context Broker – Orion Context Broker, a user subscribes to a service related to monitoring data collected and processed by the DEM and retrieves monitoring data.

3. Create a VM and deploy a GE.
4. Install DEM and appropriate plugins on the VM.
5. Through Publish/Subscribe Context Broker – Orion Context Broker, the user subscribes to services related to the monitoring of VM resource usage.
6. Collect monitoring data from several VMs across multiple nodes through Publish/Subscribe Context Broker – Orion Context Broker deployed on the Master node of XIFI.

5.4.2.1 Description of Components

Chapter	Name of GE	Short description aligned to use case
Cloud Hosting	Monitoring GE - TID Implementation [19]	Data will be gathered by this GE.
Data/Context Management	Publish/Subscribe Context Broker – Orion Context Broker	A publish/subscribe context broker for gathering data.

Table 43: UC11 FIWARE GEs.

Topic	Name of Component	Short description aligned to use case
Monitoring	XIFI DEM adapters	Physical /virtual servers adapters to be installed on the infrastructure to provide monitoring data gathering, on node and federation level.

Table 44: UC11 Self developed parts, SEs.

Other technical aspects: N/A.

5.4.2.2 Requirements to nodes / other work-packages within XIFI

As stated above, the starting point of this scenario is that a node has already joined the XIFI federation (cloud resources have been verified, initial testing has been successfully applied and FI-WARE Cloud Hosting GEs have been deployed). It should be noted that this showcase has clear dependencies with work performed in WP2, WP3, and WP4. No specific hardware or software requirements are needed for the deployment of GEs and components for this showcase.

5.4.3 Release plan

1st Release at M12:

The first release of this showcase will include the installation of the DEM monitoring components developed within XIFI and the retrieval of monitoring information on node level. Thus, the first release will be demonstrated on a single XIFI node.

2nd Release at M24:

Apart from the demonstration tasks described in the previous section (1st release), the second release of this showcase will include the retrieval of monitoring information at a federation level. Thus, the second release will be demonstrated on all XIFI nodes.

6 SHOWCASES ON INNOVATION PATHWAY

The purpose of these showcases is to demonstrate in the first instance the process whereby trials and experiments in a different environment can be migrated to XIFI, and thereby benefit from the capacity as well as market-readiness that XIFI would allow them to investigate. In addition, they show the use of other, complementary resources in connection with XIFI. In both cases, final results would not be expected until the second year since there is some investigation to be carried out in the first year in preparation for the complete showcase. The showcases for T6.4 position XIFI firmly within the overall FI ecosystem and begins to set out a clear path for XIFI working together with research infrastructures in taking work from that environment to benefit the community at large.

6.1 UC12: Migrating an existing experiment from FIRE to XIFI

Partners	IT-INN
Domain	Experimentation scaling up
Stakeholders	Developers
Relevant XIFI aspects	Demonstration of support for large scale experiment.
Adopted Enablers	DCRM GE.

Table 45: UC12 Summary table.

6.1.1 Showcase description

This task provides a showcase to demonstrate the value of XIFI as a test facility, federated with and complementing other facilities like FIRE, by plugging the gap between research, experimentation and real-world business deployment. The relationship with existing experimental facilities is studied and established in WP1 and WP5. This task will showcase how to enable experimenters with technology, or usability experiments to easily scale up to larger-scale business experiments inside the FI-PPP. It is important to highlight that the case itself is about the process of migrating the experiment, including its execution and the specific XIFI features used may be demonstrated elsewhere or used in a specific way as requested from the experiment. In particular the showcase will proceed as following:

- Identify a suitable FIRE experiment
- Identify what features need to be present in XIFI for the experiment to use.
- Liaise with the interested FIRE project
- Solve interoperability and scaling up issues
- Deploy the chosen experiment on XIFI.

6.1.1.1 Experiment definition and timescale

Interacting with the OFERTIE [20] project a suitable experiment has been defined. Since the OFERTIE project is still active, the description of the experiment is still in a draft state. Nevertheless the key information needed from XIFI at this stage has been acquired. OFERTIE will complete the experiment definition early next year and they will have it running some months later. XIFI will study any technical problems related with the migration of the experiment and will resolve by Month 12 (April 2014), so that it is possible to have the experiment running on XIFI sometime between Month 18 and Month 21 depending on the technical issues that need to be solved.

6.1.1.2 Experiment Description:

OFERTIE [20] is a FIRE project running experiments from MMORPG gaming trying to adjust the net settings according to the evolving state of the network and the number of participants. Different end-user profiles need different Qualities of Service and Experience. So, nowadays, it is more and more important to be able to adjust the configuration of the net in a dynamic way for to provide a personalized experience.

OFERTIE exploits some well-known monitoring techniques to get information about user behaviour as well as profiling it. The profiling is used to detect possible SLA violation. A specific module is then in charge of calculating the optimum configuration of the OpenFlow enabled Software Defined Network, applying it to the Openflow enabled switches.

The following picture shows the general architecture:

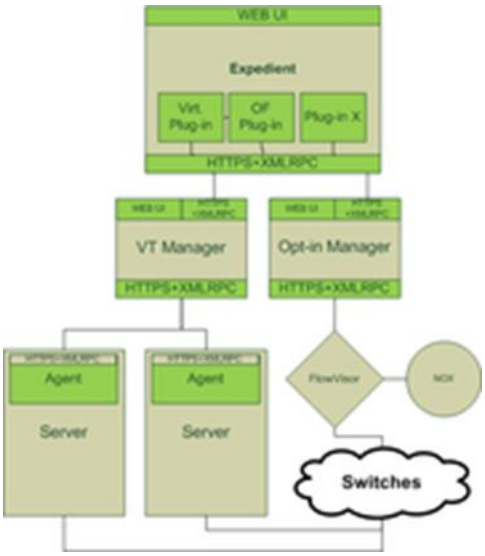

Figure 15: the OFERTIE Architecture.

OFERTIE currently uses Ofelia nodes for running the experiments and the three components used in the experiment that will be migrated are the NCL developed by I2Cat and in charge of adapting the network configuration to meet a specific Quality of Service, the Network Profiler and SLA Violation services in charge of profiling the behaviours in order to determine SLA violation.

Two different games will be used in the experiment: MineCraft [21] and Quake Urban Terror [22]. These games are OpenSource based and it is possible to freely install them. They also have an active community behind that will potentially support the experiment execution. Optionally several bots may also be installed on a different XIFI node for monitoring and controlling complete end to end quality of service. The involvement of communities provides real usage of the net with a real human behaviour that is very difficult to simulate. The following image shows the experiment architecture. It is important to highlight that with real users it is possible to monitor and control only a part of the end-to-end quality, while, by using bots, XIFI features allow control of all the connections.

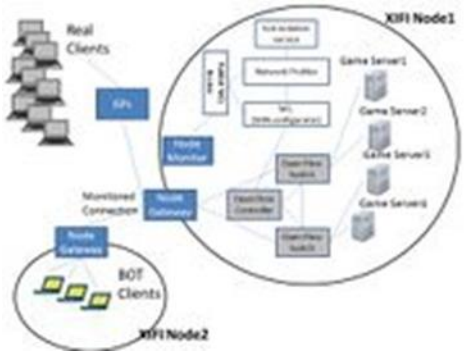

Figure 16: Experiment Architecture.

6.1.2 Requirements

The technical requirements for running the experiment will be finalized via discussion with the OFERTIE project. The following list has to be considered as a draft:

- At least four different virtual machines
- A Software defined network fully supporting OpenFlow and including at least 3 switches with the possibility of controlling them
- A standard OpenFlow interface for controlling the SDN
- A monitoring service able to monitor the SDN inside the node. This monitor should expose in a machine readable way its result to custom module installed inside a node
- a monitoring service able to control the traffic between nodes in the scenario where bots are still being used.

6.1.2.1 Description of Components

Chapter	Name of SE	Short description aligned to use case
Cloud Hosting	PaaS Manager GE	To allow Use Case project developers to register and upload SE. To allow infrastructure owners to deploy the SE in the node. To publish new instances.
Cloud Hosting	DCRM GE	To host services used in the experiment.

Table 46: UC12 FI-WARE GEs.

Topic	Name of Component	Short description aligned to use case
Monitoring	Custom modules interacting with the XIFI monitoring service	

Table 47: UC12 Self developed parts, SEs.

Other technical aspects: N/A.

6.1.3 Release plan

1st Release at M12:

The first version will prove the possibility of running the chosen FIRE experiment on XIFI having solved any migration and interoperability issues at least at theoretical level.

2nd Release at M24:

This version will support the full execution of the experiment on XIFI.

6.2 UC13: Augmented Mobile Tourist

Partners	TI
Domain	Experimentation scaling up
Stakeholders	Developers, End Users / Adopters
Relevant XIFI aspects	Demonstration of support for large scale experiment.
Adopted Enablers	Publish/Subscribe Context Broker GE, Semantic Annotation GE

Table 48: UC13 Summary table.

6.2.1 Showcase description

6.2.1.1 Motivation

Smart mobility, mobile tourist customer and proactive services augment customer experience using mobile devices with connectivity to the Internet and various sources of data ("plain" and semantic). A mobile customer travelling around an unknown city receives various auxiliary services such as audio guides, navigation, AR-views, etc. helping them discover the city and its highlights. The XIFI project providing access to various Future Internet enablers and their reach functionalities is a perfect set-up to build and run such a complex service scenario as described above: using mobility services, context-aware, and enriched with lots of content running in real-time or near real-time.

6.2.1.2 Scenario

A tourist hanging around an unknown city with a smartphone connected to a cellular mobile or wireless network with Internet access receives contextual information regarding any close-by objects: monuments, museums, buildings, etc. explained in different ways: over headphones for audio guidance and musical audio-content, video-content show as a video stream, played video clip or pictures, including additional multimedia content over the smartphone screen as augmented-reality, and even receiving navigation guidance to the nearest monument or in accordance with the tourist's own interests, preferences and recommendations from his social network friends. In this way an unknown city becomes familiar and gains special value for a customer from both perspectives: his personal interests (accordingly to the contextual information) and educational travelling experience taken from multimedia content regarding the city.

Figure 17: Example.

Actor	Role	Role description	Benefit
Tourist	Main consumer of the service	Travelling around the city with a mobile smartphone connected to Internet over a cellular mobile or wireless network	Discover a city in line with the preferences and following recommendations by friends from a social network
Telco (Mobile Network Operator)	Wireless network provider for localization service and data traffic, at least. Other add-on services are possible	Provide mobile network able at least to localize the customer and provide traffic data connection to the tourist for the information (audio, video, phone, etc.)	Increase the data traffic and provides other value-add service to the customer
Tourist infrastructure of the city (tourist city administration)	Manages tourist interests (monuments, museums, building, etc.) in city	Provide access to tourist interests in order to: obtain relevant information and stimulate or support different service contracts	Attract tourists to the city's tourism infrastructure
Tourist interests (monuments, museums, buildings, etc.) owners or managers	Manages the tourist interests	Provides access to tourist objects and to already existent multimedia data. Stipulates service contracts with the service providers	Attract tourist traffic to the tourist targets and increasing revenue of them, advertising in a positive way the object
Service provider or intermediary	These could be the Telco or city administration or any other 3rd party	Provides end-to-end service managing all aspects of the service from advertising to the multimedia delivery to the customer	Creating win-win scenarios (value chain) between different actors and taking its financial dues from the revenue chain

Table 49: UC13 actors, roles and benefits summary.

6.2.2 Technical description

- Network connectivity: 2.5G-5G, WiFi, with data traffic capability, capillary covering the city
- Quality of Service: real-time stream with no lost or delayed information and sufficient broadband width
- Mobile terminal: smartphone with large multimedia screen and basic sensors, at least for location
- Tourist interests: existing multimedia databases regarding the object or at least possibility to digitalize the content (photo or the pictures, TV transmissions of documentary, etc.)

6.2.2.1 Description of components

Chapter	Name of GE	Short description aligned to use case
Data/Context Management	Publish/Subscribe Context Broker GE	For retrieval of context data (location, social, etc.)
Data/Context Management	Semantic Annotation GE	For inference of the semantically meaningful data or from semantically tagged data

Table 50: UC13 FI-WARE GEs.

Topic	Name of Component	Short description aligned to use case
Authentication and Authorization	Authentication and Authorization service	For authentication of entities and authorization access to the services (OAuth based)
Social Network	Social Network Connector	For accessing customer information in Social Networks (FourSquare, Facebook, Twitter, etc.)
Geo-localized information	Points of Interest (PoI) Aggregator	For aggregation of place and event information (from e.g. Pagine Gialle/Directory, Google, Facebook places, FourSquare, etc.) thanks to algorithms and parameters
Geo-localized information	Recommender	For pushing potentially relevant information (e.g. events) regarding customer preferences (e.g. social)
Augmented Reality	Augmented Reality Platform	For providing enriched content to the customer based on their context (location, preference, social, etc.)
Content Management	Content Manager	For enrichment and storage of the content (User-generated and professional)

Table 51: UC13 Self developed parts, SEs.

Other technical aspects: Mobile terminal agent developed for Android allowing content (UGC) to be published and context information gathered from mobile terminal. Context Broker and Content Manager as web services will be integrated into the scenario.

6.2.2.2 Requirements to nodes / other work-packages within XIFI

The GEs listed should be installed in Trento nodes or available from FI-WARE testbed.

6.2.3 Release plan

1st Release at M12:

First version within a single node (Trento) and limited functionality.

2nd Release at M24:

Second version across more nodes and enriched functionalities.

7 CONCLUSIONS

This document has presented showcases which will be developed in XIFI to demonstrate specific features and services introduced by the XIFI federation. These showcases target FI stakeholders, such as trial application stakeholders and participating infrastructures. They are small scale and self-contained developments that FI stakeholders will use to understand XIFI's benefits and use. The role of showcases is extremely important to:

- Create training material on the usage and participation in the XIFI federation in the context of FI-Lab. The focus in this case will be more on developers, technology providers and infrastructure owners.
- Support marketing activities towards stakeholders beyond the "hands-on" developers, technology providers and infrastructure owners covered in Training activities.

In relation to the support for marketing activities, showcases will be documented through a collection of business oriented white papers that will briefly describe their benefit and coverage for the different stakeholders. White papers will be collected and navigable on the XIFI web site to facilitate dissemination of XIFI results. As regards the training material, in collaboration with WP7, the consortium has decided to collect all the training documents into a single platform, shared among all FI-Lab contributors, to provide a more consistent message to developers and other stakeholders identified for training material. Further details about the status of both these activities will be documented in D6.2 “XIFI Showcases Demonstrators v1” (M12).

Showcase implementations will be demonstrated in a first version in D6.2 “XIFI Showcases Demonstrators v1” (M12).

REFERENCES

[1] WebRTC (Web Real-Time Communication). [Online]. http://www.webrtc.org

[2] Publish/Subscribe Context Broker - Orion Context Broker. [Online]. http://catalogue.fi-ware.eu/enablers/publishsubscribe-context-broker-orion-context-broker

[3] S3C. [Online]. http://catalogue.fi-ware.eu/enablers/s3c

[4] Location - LOCS. [Online]. http://catalogue.fi-ware.org/enablers/location-locs

[5] PaaS Manager - Pegasus. [Online]. http://catalogue.fi-ware.org/enablers/paas-manager-pegasus

[6] Software Deployment and Configuration. [Online]. http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/FIWARE.OpenSpecification.Cloud.SDC

[7] OpenStack homepage. [Online]. https://www.openstack.org

[8] Store - WStore. [Online]. http://catalogue.fi-ware.org/enablers/store-wstore

[9] A Path Computation Element (PCE)-Based Architecture. [Online]. http://tools.ietf.org/html/rfc4655

[10] A PCE-based Architecture for Application-based Network Operations. [Online]. http://tools.ietf.org/html/draft-farrkingel-pce-abno-architecture-07

[11] OpenNaaS homepage. [Online]. http://opennaas.org/

[12] Network Active Monitoring (NAM) Adapter. [Online]. http://wiki.fi-XIFI.eu/XIFI:Wp3:Components:NAM

[13] IaaS Data Center Resource Management GE. [Online]. http://catalogue.fi-ware.org/enablers/iaas-data-center-resource-management-ge-ibm-implementation

[14] SAML (Security assertion markup language). [Online]. https://www.oasis-open.org/committees/security/

[15] Identity Management - KeyRock. [Online]. http://catalogue.fi-ware.org/enablers/identity-management-keyrock

[16] "XIFI Deliverable 2.2, "APIs and Tools for Infrastructure Federation v1",". [Online]. https://www.fi-xifi.eu/publications/deliverables.html

[17] Security Monitoring. [Online]. http://catalogue.fi-ware.org/enablers/security-monitoring

[18] Datacenter & Enablers Monitoring (DEM) adapter. [Online]. http://wiki.fi-XIFI.eu/XIFI:Wp3:Components:DEM

[19] Monitoring GE - TID Implementation. [Online]. http://catalogue.fi-ware.org/enablers/monitoring-ge-tid-implementation

[20] The OFERTIE project homepage. [Online]. http://www.ofertie.org

[21] Minecraft homepage. [Online]. https://minecraft.net/

[22] Quake 3 Urban Terror homepage. [Online]. http://www.urbanterror.info/home/

[23] FIWARE Store GE Specification. [Online]. https://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/FIWARE.OpenSpecification.Apps.Store