Grant Agreement No.: 258378

FIGARO

Future Internet Gateway-based Architecture of Residential Networks

Instrument**:** **Collaborative Project**

Thematic Priority: **THEME [ICT-2009.1.1] The Network of the Future**

Requirements Document

Due date of deliverable: 30.06.2011

Actual submission date: 30.06.2011

Start date of project: October 1st 2010 Duration: 36 months

Project Manager: Henrik Lundgren, Technicolor R&D Paris

Revision: v.1.0

Abstract

This document identifies and describes the main functional and technical requirements for the envisioned overall FIGARO architecture. These requirements include those identified to date in the project. This document will be used as a basis for subsequent work as input to the design and implementation of the FIGARO architecture.

Project co-funded by the European Commission in the 7th Framework Programme (2007-2013)		
Dissemination Level		
PU	Public	✓
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Document Revision History

Version	Date	Description of change	Editor	Authors
V.1.0	30.06.2011	Final version submitted to the EC.	TRDP	All partners.

Table of Contents

1 INTRODUCTION

This document describes the main functional and technical requirements that should be taken into consideration when designing the FIGARO architecture. We largely follow the methodology as described in ANSI/IEEE 1471-2000, "Recommended Practice for Architecture Description of Software-Intensive Systems" [1], here just called IEEE 1471. In IEEE 1471, architecture is defined as the fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution. IEEE 1471 provides definitions and a meta-model for the description of an architecture. For this deliverable D1.1, the most relevant notions from IEEE 1471 is that an architecture should address a system's stakeholders' concerns, and that architecture descriptions are inherently multi-view. A view is defined as a representation of a whole system from the perspective of a related set of concerns. In essence, IEEE 1471 states that no single view adequately captures all stakeholders' concerns. Therefore, before designing an architecture, the stakeholders and their concerns should be known first. This knowledge is best obtained by identifying the relevant use cases. More specifically, in this deliverable we derive FIGARO's main functional and technical requirements based on our FIGARO vision [7][8] and a rich set of use cases. We focus on the requirements that are key to the architectural work to be carried out in FIGARO. More detailed use cases and requirements can be found in the more topical deliverables of the project [3][4][5][6].

The remainder of this deliverable is organized as follows. Section 2 recapitulates the FIGARO vision. Section 3 provides a distilled overview of the considered use cases. Both the vision and the use cases are the basis for our requirements that we discuss in Section 4. Finally, we conclude this deliverable in Section 5.

2 FIGARO VISION RE-CAP

The Internet has evolved from a technology-centric core network to a user- and content-centric scenario that must support millions of users creating and consuming a variety of content and applications. It must be able to accommodate new services with diverse requirements while coping with heterogeneous networks and systems.

Our work is driven by the identification of the following main overall challenges. First, residential networks connected at the edge of the Internet are becoming a more complex, yet more important integral part of the Internet. These residential networks are typically controlled by non-technical end-users, which give rise to new challenges in terms of simple network management for regular end-users. Functionality alleviating the users' burden of manually configuring, monitoring, and optimizing their networks, as well as aiding users in case troubleshooting, needs to be added to residential networks. Second, new networking mechanisms are needed to better support the users having easy remote access from the Internet to their residential networks and their content/services traditionally residing in the cloud. Third, following this, the Future Internet must include an improved support for the users to easily handle their digital content. Improved content management needs network architecture support to efficiently provide storage, search, and access of digital content. Furthermore, the content should be easily accessible regardless from where the users are connected to the Internet. It must also guarantee content privacy as well as easy content sharing, depending on content type and the owners' preferences. Fourth, the support for community-oriented networking must be improved in the Future Internet. Innovative systems and network solutions must be developed to better support and exploit community networks to provide improved value-added services to the users. Finally, the

integration of other sectors with the Future Internet poses challenges for how to interconnect different networks and systems that do not necessarily use IP technology, to ultimately provide a common service infrastructure. Moreover, the user interaction with these services must also be revisited for a successful integration. The major challenge is therefore to design a network architecture that addresses these challenges.

The FIGARO Approach

Like today's Internet, the Future Internet will consist of separate domains controlled by different entities, such as operators, enterprise's IT departments, etc. Within these domains, functionality is often distributed according to well-known network design paradigms. For interconnecting these domains, a crucial role is given to border gateways. One of the most important border gateways is possibly the home gateway, interconnecting the residential domain with an operator's domain. FIGARO recognizes the increasing importance of the role of the individual in his/hers living environment in using and creating Internet content and services. FIGARO therefore proposes a Future Internet architecture that is structured around the residential networks connected at the edge of the Internet. The fundamental concepts of FIGARO and its overall architecture are *gateway-centric networking* and *federation of residential networks*. In this architecture, federated home gateways have a key role. As "always on" devices, they do not only provide connection to the Internet, but also enable aggregating a multitude of devices and services, and efficient management of networks, content, applications, and services.

In FIGARO, residential gateways undertake the federator role, internally as well as externally. Figure 1 shows residential networks connected at the edge of the Internet and illustrates a simplified view including the two types of residential network federation. The upper part illustrates external federation interconnecting multiple gateways to form a cooperative overlay across residential networks. This federation enables further collaboration to offer added value in terms of, for example, access and sharing of content, storage and network capacity. The right-most residential network illustrates an

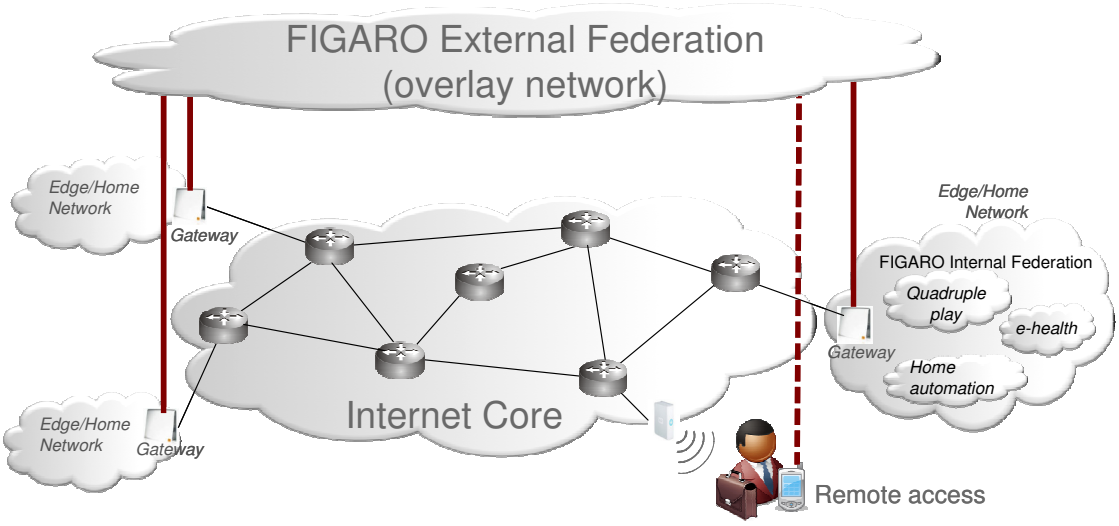

Figure 1. FIGARO gateway-based external and internal network federations.

example of an internal network federation consisting of the regular IP-based network on one hand, and other types of networks, possibly non-IP, specific to services in other sectors (e.g., home automation and e-health). The federation enables features such as communication, resource, and content sharing among the involved networks as well as a common interface to these networks through the gateway.

FIGARO will develop a gateway-centric network system architecture including the following components.

- *A network organization and optimization framework* that can exploit gateway-centric federation among internal networks as well as across federated neighborhood community networks.
- *A content management framework* that enables distributed content backup, search and access.
- *New management and control modules for a common service delivery infrastructure* by extending current intra-sector control and interface platforms.
- *A network monitoring framework* that can characterize network and application performance across its networks.

3 USE CASES OVERVIEW

In this section we provide an overview of the use cases we consider in FIGARO. We focus on the use cases most relevant to our overall future FIGARO architecture. Rather than describing all these use cases in great detail, in this deliverable we try to group and abstract these use cases whenever possible. More detailed use case descriptions and requirements can be found in the more topical deliverables of the project [3][4][5][6]. The use cases are grouped along the lines of the technical aspects they relate to most.

3.1 Networking

FIGARO will provide innovative networking solutions that improve network performance and end-user QoE of digital content and services. These solutions will leverage the gateway for network federation and content-awareness. We consider the following main use cases:

- **Federated neighbourhood network optimizations**.

  We group all the use cases that exploit external federation under this use case. This includes a set of networking services that use the same fundamental federation concept, but utilize it in different ways and/or for different purposes.

  - *Backhaul bandwidth aggregation*. This use case is based on client devices that can connect to multiple neighbouring APs and exploit their (unused) access network bandwidth to increase performance.
  - *Wireless neighbourhood optimization.* The federated neighbourhood network collaborates in exchanging monitoring data and performing wireless network optimizations (e.g., interference mitigation) to improve performance.
  - *Load-balancing.* The client associations to APs are load-balanced across neighbouring APs for improved performance.
  - *Eco-management*. The client associations to APs are managed across the neighbourhood such that a maximum number of gateways can be turned off to save power, after offloading their clients to neighbouring APs.

- **Remote access**.

  We group the cases that include some type of remote access under this use case. The two main cases from a networking point of view include:

  - *"Foreign" federation gateway access*. This use case leverages the federation to connect to other federated gateway to exploit resources. This can be done to gain access to the Internet (c.f. FON [9]), but, more interestingly, can also be used to exploit other resources such as computation and storage.
  - *Remote access to home network and its content/services*. This can be realized either through any Internet connection or through the connection to a "foreign" external federation gateway (this may allow for different functionality).

- **Gateway-assisted video streaming optimizations**.

  This includes two different use cases.

  - *Transparent multi-path adaptive video streaming.* This use case leverages the home gateway to improve video streaming services by, transparently for the end-user, implementing multi-path transport support between the service provider and the home gateway. This provides improved robustness and performance.
  - *Video-aware wireless optimizations.* This use case leverages the gateway to exploit information about the video stream characteristics and optimize the wireless network for improved end-user quality of experience.

3.2 Content Management

FIGARO will provide a new distributed content management architecture. This architecture will leverage the gateway's central position in the home network and its connection to external federation networks and the cloud. We illustrate it with three main use cases.

- **Unified content access.**

  End-users should be able to transparently access content across all home networking devices, independent of their underlying file system technology. The gateway will provide a unified catalog of all content in the home network by offering content management service along with a unified distributed virtual file system.

- **Gateway-assisted content management.**

  There are three main use cases related to gateway-assisted content management services.

  - *Cloud storage integration.* This use case extends the unified content access, by including cloud storage. The gateway transparently (from the user) handles the access to the end-users' cloud storage services. This supports storing content as well as accessing (consuming) content as it would be locally in the home network.

  - *Backup service*. This use case provides secure backup of content in the external federation network. A backup service runs in the home gateway. It cooperates with the gateway's content manager to have access to all the content in the home network (through the unified content access) and to decide which content to back-up. It then collaborates with other federated gateways to offer data backup service for each other.

- *Social-aware content sharing*. This use case exploits information, collected from the social networks that home users are part of, in order to combine content sharing and content caching/backup. For example, in the case of a set of pictures, content tagging done by the content owner (e.g., friends, family, colleagues) is used by the gateway to decide on which federated gateways to share/cache the photos, depending on social preference of remote users on such federated gateways.

- **Remote content access.**

  This use case specifically involves unified access to the content stored in the home network from a remote location providing Internet access.

3.3 Converged Services

FIGARO will deliver new management and control modules for a common service delivery infrastructure by extending current intra-sector control and interface platforms to a single cross-sector platform. We will leverage the reliability, control, and interface provided by the home gateway. We will explore the integration of applications and services from the ICT sector with other sectors, such as energy management, home automation and e-Health. We group the use cases under those three topics.

- **Energy management**

  The use cases for energy management focus on the gateway's role in connecting the gateway with metering devices (energy smart meter and sensors) and collecting/aggregating data and displaying this data to the end-user. It also includes the connection and control of electricity producing and energy storage devices in the home (e.g., solar panels, batteries).

  - *Gateway-assisted energy meter data collection and display.* This includes the gateway connecting to the smart meter to collect and present energy consumption data as part of an energy information service. The end-user can view the information by accessing the home gateway. The information service can be provided directly by a stand-alone application on the gateway or through interaction with an information service provider. Note that the energy service provider does not rely on home gateway, but can perform remote smart meter readings through its existing infrastructure.

  - *Power consumption measurement and display.* This includes the gateway connecting to energy sensors in the home to collect data about energy usage. These sensors can exist directly in appliances or in power outlets. The end-user can install a dedicated application on the gateway that collects sensor readings and allow viewing this information by accessing the home gateway.

  - *Gateway-assisted energy subscription services (pre-paid).* This use case focuses specifically on the integration with a service provider's subscription service. It includes the home gateway being part of a pre-paid energy subscription service, where the end-user can read subscription status (remaining credits) and manage the subscription (pre-paid refill) through the home gateway.

  - *Local virtual power plant service.* This case assumes that the homes have local electricity production (e.g., solar panels, wind mill) and potentially also local energy storage (e.g., batteries). The home gateway plays a key role by implementing part of the smart grid's logic, including data collection of energy consumed and produced, pricing models, user preferences, and interface to "smart grid service".

- **Home automation (domotics)**

  These use cases focus on user interfacing and control of home automation services.

  - *Central heating thermostat.* This includes the gateway connecting to sensors and thermostat for collecting data and controlling thermostat functions through the gateway user interface.

  - *Remote graphical user interface for control devices.* This includes the gateway connecting to home automation devices/services to provide remote user interface.

  - *Gateway-hosted advanced home automation system control.* This includes the gateway hosting an application for controlling an advanced home automation system. The gateway can connect and interface with a dedicated home automation server, or simply implement all the home automation logic itself.

- **e-Health**

  These use cases focus on the gateway integrating with e-Health services and the migration of current solutions to a common service delivery platform. This includes connecting to measurement devices using heterogeneous network technologies, providing a user interface, data collection and storage, and potentially data sharing.

  - *Gateway-assisted e-Health care service (health & fitness).* This case focuses on fitness and healthy living, using e-Health services integrated with the gateway for data collection, sharing, and display. People are in control of their health, and are enabled to proactively act on this.

  - *Ageing independently with e-Health care.* This case focuses on ambient assisted living using e-Health services enabled by the gateway, allowing elderly live longer independently at home. The gateway connects and reads data from measurement devices; this includes both health device (e.g., blood pressure meter) and surveillance sensors (e.g., cameras, movement sensors). Collected data can be shared in a controlled manner with e.g., doctors and family members.

3.4 Monitoring

Monitoring is to a large extent driven by the need of other services/use cases. Although monitoring in FIGARO therefore does not really have any independent use cases per se, we identify some important aspects of its intended operation below.

- **Network monitoring.**

  This service monitors the home network and the access network based on a set of selected performance metrics. This also includes measuring complete Internet paths to e.g., other FIGARO gateways or cloud services. The focus is on the performance of the networks. This monitoring service will provide access to monitoring data to other services and/or modules in FIGARO. It is therefore mainly driven by the requirements of these services/modules.

- **Service and application monitoring.**

  This service complements the network monitoring by monitoring the data traffic to identify active services and applications, and to track their performance.

- **Troubleshooting.**

  This service will use the monitoring data from the network monitoring and the service/application monitoring to provide a troubleshooting service. It will raise alarms and try to locate the origin of the performance problems. It can either run in an automatic manner, notifying the user via alarms, or it can be especially invoked by a user that currently has a problem.

3.5 Conclusions

In terms of stakeholders, most use cases still deal with the main three roles: an operator remaining the principal owner/controller of the home gateway, and an end user consuming services from service providers. However, our vision includes that the end-user has extended control compared to what is the case today, especially with regards to installation/start/stop of applications and services on the gateway. In addition, we envision that various new types of service providers appear in the market, which provide new services "over the top", i.e., using the operator's network and home gateway, with strict demands on the network and gateway, but without the traditional strict relationship (where either the service provider and the network operator were one and the same company, or the service provider had to deliver over an Internet connection of best-effort quality only). In the next section, the concerns of these stakeholders are represented in their translation to technical system requirements.

4 REQUIREMENTS

In this section we identify the requirements based on the FIGARO vision and use cases. The organization of these requirements largely follows the organization of the use cases in Section 3.

4.1 Networking

In this section we identify and discuss the main requirements from the networking module point of view.

The **neighborhood network federation** has the following main requirements. First, an "external federation" module that manages the connection between federated gateways must run on each gateway that is part of the federation. This module must be accessible from the Internet as well as from the gateway's WiFi interface. A lookup service must exist to locate and connect to external federation members, both over wired and wireless networks. The federation module must also export certain functionality in order to support various federation services. For example, sharing of certain monitoring data among federation members is needed to perform *wireless neighborhood optimizations*. Thus, there needs to be signaling and communication protocols for communication between federation members. Several federation related services also require virtualization of the wireless interface (e.g., through multiple ESSIDs), or the availability of a secondary wireless interface to perform signaling tasks. This is to allow and control the association and access of federation members to other members' wireless networks. This is required for the *load-balancing* and *eco-management* services where neighborhood federation members associate across each others' wireless APs. It is also required to virtualize access network interfaces, or provide isolation and bandwidth allocation (between home users and external users) by other means (e.g. traffic shaping). For similar reasons, it is also necessary to be able to manage (e.g., prioritize) network traffic based on e.g., different types of users or services. The *backhaul bandwidth aggregation* service shares these requirements, but in addition requires that end-user devices can virtualize their wireless cards in order to cycle their communication with different neighbour gateways in a slotted fashion to exploit the

backhaul network aggregation. Most of the network federation services require network monitoring. For example, wireless neighborhood optimizations require detailed monitoring of wireless settings and wireless network performance (bandwidth, packet loss, delay, busy time, etc.). Load-balancing, eco-management, and backhaul aggregation require similar monitoring data, but also monitoring of the access network.

The **remote access** has two basic requirements. First, in the first case of *"foreign" federation gateway access*, it requires that federation members have access to other members' wireless APs. If this access is used to enable certain federation services, then this federation access must be able to associate with the "federation overlay network". Second, for *remote access to home network* the gateway must support VPN. VPN pass-through on the gateway is required to connect to/from a specific device in the home network. Any type of "foreign" access to other federation members ultimately requires authentication and authorization. Although content being transmitted over the remote access service may be encrypted, we still require that the VPN has encryption support for communication over a secure channel.

The **gateway-assisted video streaming optimizations** have the following main requirements. *Transparent multi-path adaptive video streaming* requires support for multi-path communication (e.g., SCTP or MPTCP). Multi-path can be implemented with a number of different network topologies wherein the gateway, the service provider or both are multi-homed, thus providing at least two distinct network paths. Our basic configuration includes multi-homing of video server, and an HTTP proxy at the gateway to trigger multi-path communication. Further throughput and reliability improvements can be achieved if the gateway too is multi-homed. Gateway multi-homing can therefore be considered an optional requirement. Gateway multi-homing can be achieved through the addition of a WiFi interface used for accessing federated neighbourhood gateways, or via a separate access network (e.g., cellular). *Video-aware wireless optimizations* leverage information about the video stream and must therefore be able to obtain video stream characteristics (e.g., streaming bitrate) either through video stream identification or monitoring in order to perform its optimizations.

We summarize the requirements in the list below.

- An external federation module on each gateway that supports well-defined signaling and communication protocols.
- A federation gateway look-up/tracker service.
- Authentication and authorization[1].
- Wireless network virtualization at home gateways, and in special cases on client devices.
- Secure VPN support at home gateways.
- Multi-path networking support at video servers and home gateways. The gateway may host an HTTP proxy or, alternatively, may be multi-homed.
- Multiple WiFi interfaces may be required for certain services to perform optimally, namely the eco-management and the multi-path adaptive video streaming service.
- Network modules must be able to access detailed network monitoring data from the home network and the access network.
- The external federation module must be able to access and share certain monitoring data with other federation members (gateways).
- Virtualization to provide isolation, management, and control of resources.

[1] We assume that an Authentication, Authorization, and Accounting (AAA) service exist in the service provider network, but we still want to point out the need for authentication and authorization in our federated networks.

- Sharing of content characteristics between content storage/management modules and networking modules.

Further and more detailed requirements will be discussed in Deliverable D3.1 [4].

4.2 Content Management

In this section we identify and discuss the main requirements for the content management framework.

To bring the concept of **unified content access** to fruition requires mechanisms that enable end-users to transparently access all their content in a unified manner. These mechanisms must therefore be able to access content independent of location and underlying file system technology and network storage, and present it to the user in a unified manner. First, a gateway-centric solution requires functionality similar to a distributed virtual file system at the gateway that can access content across all home network devices. Thus, the gateway must implement support for the most common (network) file systems and aggregate them to a unified file system view. Next, a content management framework exploiting the unified file system view is required to provide the end-user with a unified catalog service, that implements indexing, search, and access to all content in the home network in a seamless manner. This content management/catalog must be accessible to all (most) devices in the home network, thus through a standardized protocol/interface (e.g., a web interface). Third, a management service for automatic handling storage devices joining and leaving the network (i.e., the distributed file system) is also needed to eliminate complexity for the end-user.

To extend this **gateway-assisted content management** requires more functionality. To *integrate cloud storage* in the unified content access requires open interface at the cloud storage and a module in the gateway's distributed virtual file system that implements this interface.

A *gateway-assisted backup service* requires (i) access to all home contents, (ii) a synchronization module providing consistency between local devices' resources and the local storage of each gateway, and (iii) an encryption module, with the aim of securing the local storage in the NAS. Similar to other external federation services, it also requires requires a tracker service (i.e., a per-federation dedicated server) that facilitates the look-up of and the connection to gateways in the external federation. However, in addition, it specifically requires dedicated storage on these gateways to store the backup data. Each local storage (e.g., a NAS directly connected to a gateway) has two distinct portions of space: the first for the local backup of local home network's registered users, and the second for other federated users' backups or content replication. This latter portion of space has to be accessible through the federation in order to store encrypted file fragments coming from different backup modules running on the federated gateways, as well as shared content (see below).

A *social-aware content sharing* function requires the end-user being able to "tag" content in some manner. It also requires mechanisms to map the content (via their tags) to interests of users in the end-users social network, and then in turn map this to the federation (in case the social network and the federation are not identical). Similar to the backup services, the content sharing needs a tracker service to look up and contact federatioed gateways. However, in contrast to requiring a personal storage, the content sharing services requires storage space that is shared among a set of (or all) users in the federation.

Remote access to the home content requires a (secure) connection to the content management system on the home gateway. Assuming an HTTP-based solution for access to the content management system, the gateway must run an HTTP server with SSL encryption support. An optional requirement is for a remote device to appear in the distributed virtual file system and thus expose its content through the content management system. This requires VPN support in the gateway and integration of VPN support in the distributed virtual file system. Another optional requirement is to remotely consume content using DLNA/UPnP, which requires a (secure) VPN connection to the home network and DLNA/UPnP enabled devices. In all cases, remote clients must know how to connect to the home

gateway, which requires a look-up service.

We summarize the requirements in the list below.

- A distributed virtual file system for aggregating the content in all different home network devices to a unified file system view.
- A unified content catalog service for seamless content indexing, search and access that operates on top of the unified file system view.
- Standard access to the unified content catalog service not requiring software installation on end devices..
- A network file system manager that handles the join/leave of devices belonging to the virtual file system.
- Open interface cloud storage services.
- Cloud storage file system interface modules in the gateway's distributed virtual file system framework.
- Terabyte-scale storage to allow for storing, sharing and backing-up content.
- A data backup module on the gateway.
- Data encryption capability on the gateway.
- A federation gateway look-up/tracker service (same as for all federation services).
- Authentication and authorization.
- Dedicated storage space on "foreign" federation gateways.
- Support for customized content tagging.
- Storage space that is shared across federation members.
- Secure remote access to the content management system on the home gateway.
- The distributed virtual file system may require support for VPN connected devices.

In addition to the requirements above, a content management framework is being described in Deliverable D4.1 [5].

4.3 Converged Services

This section summarizes the requirements that were previously identified and discussed in the Deliverable D5.1[6]. In addition, we also include the summary of its discussion on design considerations as input to our requirements.

Many of the services from the "other" sectors we consider in FIGARO (energy management, home automation and e-health), typically have stronger requirements on reliability, security, and access control. This requires special attention when integrating these services with the home gateway (and potentially with other services on the gateway). A key role of the gateway for the converged services is that the gateway can connect to the network and the devices of these services. Since Zigbee is a widely adopted technology in these sectors, support of this technology is a specific requirement. It is also necessary that the gateway can act as a remote user interface for devices with limited interface capability. Since different sectors are considered, the gateway must also support hosting applications and/or interfacing/integrating with services from different service providers. This requires a secure and flexible execution environment that provides isolation.

We summarize below the discussion on design considerations from Deliverable D5.1[6].

Loosely-coupled integrated control using information brokering

We propose that technical sub-systems in homes are functionally integrated through the use of an information brokering system. This information brokering system would provide services for sub-systems in homes, including service discovery and query/response, publish/subscribe like services. Home services may publish events or data, other services may use the data. For instance, an alarm clock could – upon being set by a home resident – publish this fact and the wake-up time. It does not need to be involved further. A heating system can then access this kind of data (wake-up, leave home, etc.) and determine its behavior based on that information. Other systems may do the same. In this way, systems are loosely-coupled, failure of one of the providing or consuming sub-services, would then not have to result in failure of all functionality.

Graceful degradation of integrated services

Integrating functions and services must be designed such that basic services remain operational even during (partial) failure of the network, networked devices or services. In other words, even if the *integrated* functionality is no longer available, the basic functionality must be. For instance, if a heating system is to operate in a networked setting, it must maintain the basic functionality of heating a home, even if a home gateway that would provide mobile access to home residents, for instance, is unavailable. If the gateway, and the connection to the heating system, is restored again, only then can users use their mobile devices again for setting the heating.

Support for multi-vendor systems, multiple service provider, multiple gateways / home

The architecture to be designed and developed should support multiple gateways of multiple vendors, using multiple service providers, in one home. Although integration at the gateway level would be a primary objective for integrated services, the architecture should support that a consumer may use multiple over-the-top gateways. A gateway may be delivered as part of a service of a service provider, and a consumer may use another service from another service provider, that includes a gateway device as well. This should work in a single residential environment, regardless of the number of gateways, their make, or the service provider that provides (services for) them.

Security and privacy

Federations of gateways must have an architecture that respects the security and privacy of home residents. Whereas sharing of information enables additional use cases, ultimately, the home resident must be able to stay in control of the information that is shared on his behalf, or services that are accessible on his behalf. At any time, the home resident must be able to revoke authorization and access to services and information that he/she has made available, in a simple way.

Distributed connection management for federated gateways

Gateways that are to be federated should not become too dependent on centralized coordinating systems. They may become a single-point-of-failure and a bottleneck in busy times. A federation controller should therefore provide minimal services to the members of the federation. For instance, it will put the members in touch with each other, however, it will let the members of the federation communicate directly, and not sit in between members, or keep a detailed state of the communication.

We list the main (and most common across these use cases) requirements below

- The gateway must have at the minimum one Zigbee interface.
- The gateway should act as a Zigbee bridge and be able to connect to any Zigbee device or network.

- Gateway-based services should be available through remote access (VPN).
- Services and data have to provide security measures to ensure privacy and content confidentiality.
- Critical services must have strong access control.
- Support for Authentication, Authorization, and Accounting (AAA) is required.
- The gateway has to allow hosting applications from different service providers. This requires a flexible and isolated execution environment.
- The gateway should support different services to share data.
- The gateway should be able to discover devices and their capabilities.
- The gateway should provide a user interface for (constrained) devices.
- Critical services must be designed for high reliability and without single point of failure.
- Graceful degradation of integrated services (distributed, loosely coupled, decomposed).

4.4 Monitoring

This section collects the requirements for the monitoring functionalities that stem from the other FIGARO modules/services.

Recall that the monitoring framework includes three main components: a network monitor, a service and application monitor, and a troubleshooting service. The first one provides monitoring of the various networks' status and performance. This includes wireless networks (WiFi, Zigbee, etc), wired in-home networks (Ethernet, PLC, etc.), and broadband access network. It also includes probing full Internet paths to other FIGARO gateways and/or cloud resources. Although it is possible for a monitoring service to collaborate with end-user devices, in FIGARO we consider a gateway-based monitoring framework. That is, we require network monitoring on the gateway's network interfaces. While the complete set of metrics will be provided in Deliverable D2.1, we list here a core set of metrics needed by our main networking services.

Furthermore, the gateway should store the monitoring data in a well-defined format and must provide a well-defined API for (read) access to the monitoring data. The monitoring API should also support access to data in aggregation format such as data statistics. An efficient database requires low processing power and moderate storage. It is also required that other services/modules in the gateway can access monitoring data. However, similar to other content, monitoring data must be protected by authentication and authorization.

Service and application monitoring should be able to study data traffic that passes through the gateway and infer which services or applications that certain traffic flows belongs to. The processing power for online techniques is high, wherefore hard real-time operation is not a strict requirement.

The troubleshooting service must be able to access monitoring data. It must be allowed to perform additional active measurements in order to infer the location of performance problems.

We summarize the monitoring framework requirements in the list below:

- Network monitoring must be supported on the gateways network interfaces, including access network.
- Network monitoring should support probing of full Internet paths.
- Network monitoring should be non-intrusive and not disrupt other traffic in the home network noticeably.

- The monitoring module should provide short convergence times and limit the reporting delay to orders of seconds for one-shot metrics such as interface statuses or simple RTT and reachability measurements. For continuous and complex measurements such as application monitoring or topology mapping higher response times are acceptable.
- Monitoring data should be stored in a database.
- Monitoring data must be accessible through a well-defined API.
- The monitoring API should support data aggregation.
- Monitoring data must be accessible by other functional modules (e.g., networking modules, content management modules, etc.).
- Service and application monitoring should be able to study data traffic that passes through the gateway.

While the complete set of metrics will be provided in Deliverable D2.1, we list here a core set of metrics needed by our main networking services.

- Wireless network capacity, available bandwidth, busy time, and packet loss as well as detailed information about the wireless neighborhood environment (which APs, their configuration, their traffic load/pattern, and perceived signal strength).
- In-home wired network characteristics, such as throughput, available bandwidth, and packet loss.
- Broadband access network characteristics, such as throughput, available bandwidth, and packet loss.

Further requirements including the specification of metrics and data formats will be detailed in Deliverable D2.1 [3].

4.5 Additional System Aspects

In this section we identify and discuss additional system aspect requirements.

- We assume that our FIGARO gateway is equipped with most (all) standard networking technologies. However, we wish to highlight specific network interface requirements. The home gateway must have a Zigbee interface and be able to act as a Zigbee bridge. This is a requirement for most current energy/home automation/e-health services. Although such services may over time migrate to IP, we keep zigbee as a requirement at this phase of the project. The Zigbee interface may be a USB dongle.
- We consider that our gateway may be a hybrid gateway that implements both gateway functionality as well as set-top box functionality. As such our gateway may be equipped with video output.
- Based on our estimations of the requirements from the various services and modules we consider in this project, we target a gateway with a powerful atom processor (2GHz range), a few giga-byte of RAM, and a few tera-byte storage. The processing and memory requirements mainly stem from the need for a flexible virtualized execution environment to host a wide range of services. The storage requirements mainly stem from content management, where the gateway should be able to host content for e.g., backup services as well as content sharing and caching. These requirements are just slightly above what exists on the market today, and is a reasonable target a few years from today.
- The gateway architecture has to be modular, well decomposed, and with well-defined APIs.

This is a necessity for realizing a gateway-based architecture with such a rich set of services, and integration of different services or functionalities. Furthermore, such a modular architecture with open APIs is also an enabler for multi-vendor support.

- It is also clear from several use cases that the FIGARO gateway needs a secure and flexible service hosting execution environment. We have identified that some kind of virtualization is needed to address (part of) this requirement. More details on virtualization will be given at a later stage in the project.

5 SUMMARY

In this deliverable we have briefly recapitulated the FIGARO vision and overviewed the core use cases considered by the project. These in turn have been used to identify a set of requirements that are important in our future work to design the FIGARO architecture. We have deliberately focused on consolidating those requirements that need to be considered for a sound grounding of the upcoming FIGARO architecture design. We have deliberately left out detailed or implementation specific requirements in favor of readability and conciseness, and kindly refer the reader to other project deliverables [3][4][5][6] for additional information related to such requirements. This document provides a list of requirements that will be used as a basis for subsequent work to design the FIGARO architecture. The project will deliver a first version of the FIGARO architecture decomposition in Deliverable 1.2 [2].

6 LIST OF ACRONYMS

AAA	Authentication, Authorization, Accounting
AP	Access Point
DLNA	Digital Living Network Alliance
API	Application Programming Interface
FIGARO	Future Internet Gateway-based Architecture for Residential netwOrks
ICT	Information and communication technologies
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
MPTCP	Multi-path Transmission Control Protocol
NAS	Network-Attached Storage
QoE	Quality of Experience
PLC	Power Line Communication
RAM	Random Access Memory
SCTP	Stream Control Transmission Protocol
UPnP	Universal Plug and Play
USB	Universal Serial Bus
VPN	Virtual Private Network

7 REFERENCES

[1] ANSI/IEEE Std 1471-2000, "Recommended Practice for Architectural Description of Software-Intensive Systems".

[2] FIGARO project, "Deliverable D1.2: FIGARO system architecture decomposition". *To appear.*

[3] FIGARO project, "Deliverable D2.1: Report on the specification of metrics and data formats". *To appear.*

[4] FIGARO project, "Deliverable D3.1: Requirements for federated network organization and heterogeneous network optimizations". *To appear.*

[5] FIGARO project, "Deliverable D4.1: Overview of the unified content management architecture". *To appear.*

[6] FIGARO project, "Deliverable D5.1: State-of-the-art of energy management, e-Health and community-service requirements on common service delivery frameworks", March 2011.

[7] FIGARO project, "Deliverable D6.1: FIGARO Project Presentation", December, 2010.

[8] FIGARO project, "Description of Work - Annex I", June 2010.

[9] FON official website, http://corp.fon.com/.