| | |
|---|---|
| Project Number: | **Contract Number: INFSO-ICT-*224287*** |
| Project acronym: | **VITAL++** |
| Project Title: | **Embedding P2P Technology in Next Generation Networks: A New Communication Paradigm & Experimentation Infrastructure** |
| Title of Report | **Mechanism for NGN operations integration in P2P communications** |

| | |
|---|---|
| Instrument: | STREP |
| Theme: | ICT-2-1.6 |
| Report Due: | M21 |
| Report Delivered: | M23 |
| Lead Contractor for this deliverable: | BCT |
| Contributors to this deliverable: | Konstantinos Koutsopoulos (BCT), Jens Fiedler (Fokus), Nikolaos Efthymiopoulos (UoP) |
| Estimated person Months: | 29 |
| Start date of project: | 1st June 2008 |
| Project duration | 30 months |
| Revision: | Version 0.1 |
| Dissemination Level: | PU - Public |

**This page intentionally blank**

# 1 Table of Contents

# 2 List of Figures

# 3 Executive summary

The design of a migration frame for P2P services in NGN networks has been driven by the concept of a gradual integration of the two inherently different technologies in the context of the identification of an optimum point between the two planes. The process of such integration involves the replacement of certain functionality in the one plane with mechanisms provided by the operation of the other. The overall target is the enhancement of IMS controlled media related services by the power offered by P2P networks and techniques.

In this essence the following main functionality areas have been identified as the main axes on which the integration should be based:

- User Authentication
- Digital Rights Management
- Content Management
- Content transfer

For the first three functionality areas IMS controlling strengths have been taken advantage of while for content transfer have been based on the P2P scalability and failure resilience.

The functional groups are integrated according to a series of principles that try to address proper content and rights management as well as operational and performance requirements.

Such integration requires adaptation of procedures and methodologies that are normally met in pure IMS or P2P application and services. Additionally, the envisaged operation is achieved by the introduction of new components that provide solutions for each the functionality areas addressed above.

Both in the client and network side associations among functional components and services, message flows and transactions have been designed in a way to allow for the realization of the project's use cases under the generic integration principles. However, as long as these principles are not violated, further deployments of the Application Server or the Client side components can be designed and tested on the basis of the offered capabilities for the provision of other added value applications.

# 4 Introduction

Although in the project's Technical Annex the work in WP3 is split between two different tasks, in the process of defining the mechanisms that will allow for the integration between P2P and IMS it became evident that there cannot be a clear border that separates the "Design of the overlay network architecture components" from the "Design of the migration frame for P2P services in NGN networks". Therefore it was decided that the overall solution is tackled with as a common task.

This has affected the way the two reports have been generated. The decision taken was to report all the technical details of the platform including server side and client side components in D3.1 whereas to present the concepts and the way the various issues were tackled with in the present document.

The current document is organised in the following way:

- Chapter 5 presents a comparison between IMS and P2P in order to summarise the differences of the two worlds and to indicate their major advantages and disadvantages
- Chapter 6 focuses on how the advantages of the two technologies can be exploited in the integrated platform by specifying functional groups for which decisions can be taken regarding the realisation approach
- Chapter 7 presents the impact on the client and server side of the decision taken as this is expressed by the modification of existing components or the introduction of new ones. The same chapter also covers issues relating to performance improvement as a result of the integration of the two technologies
- Finally, Chapter 8 summarises what the projects offers as an outcome with respect to services and client side components that can be potentially used by other parties that need to experiment or built on top of the presented IMS/P2P integrated approach

# 5 Comparison between P2P and IMS

When comparing IMS and P2P, we compare two inherently different paradigms. IMS as a technology for controlling mediaflows, administer subscribers and control access to services. IMS is a very centralistic architecture, which has its strengths in controlling. P2P technologies on the other side have been designed to be scalable and failure resilient, mainly for the distribution of media (files, streams). The following table illustrates the complementary features of both technologies, which are discussed in the following.

| | P2P | IMS |
|---|---|---|
| Scalability | Very good | Difficult |
| Single Points of Failure | No | Yes |
| Users as Content Providers | Yes | No |
| DDoS vulnerable | No | Yes |
| Access | Easy | Difficult |
| Security / AAA | Bad | Good |
| Topology aware | Difficult | Yes |
| Standardized | No | Yes |
| Quality of Service | No | Yes |
| NAT Client Problem | Difficult | No |
| Service Deployment | Difficult | Easy |

**Table 1: IMS vs. P2P comparative overview**

As already mentioned, scalability is one of the biggest features of P2P networks, while scaling up an IMS core network can only be done by configuration. P2P networks usually has no single point of failure as they are self-healing, while e.g. the HSS is a single point of failure for an IMS network. In a P2P network, users are the only content providers, while this concept is not supported in the IMS, which clearly distinguishes between consumers and service providers. Under normal circumstances, a P2P network is not vulnerable to DDoS attacks, because an attacked node will behave as a single failure, which is subject to self-healing in the rest of the network. IMS is more vulnerable, as e.g. an I-CSCF may be flooded and put out of service for all users. Access to a P2P network can be considered easy, as there is no access control in open P2P networks. Nevertheless, there exist password controlled P2P solutions, but none of them are standardized. Access to an IMS and its services is quite complex, as cryptographic mechanisms need to be deployed

for even the simplest access. Additionally, each user must be provisioned and its profile, which is stored in the HSS, must be maintained.

But in the direct comparison, IMS does not only have disadvantages against P2P technologies. The complexity of access results in a much better security situation among IMS users due to the AAA management in the IMS core network for all users. Due to the fact that IMS is located in an operator network, it can also access network topology information (e.g. from a NASS, described in more detail in D2.2), which can only be estimated or measured in a pure P2P overlay and therefore result in better overlay if presented to an overlay construction algorithm. IMS is a standardized architecture with standardized network protocols and functions, which makes development for an open market possible, while P2P overlays are usually dictated by the associated piece of software. For the same reason as for topology awareness, IMS components can influence the data paths between users and service nodes in terms of bandwidth (resource reservation), which is completely unthinkable for any pure user driven P2P network, as user nodes cannot influence routers in any of the involved networks. P2P systems usually need to provide remarkable efforts, up to dictating the architecture of the overlay, in order to make clients communicate with each other which are behind a NAT. In the IMS, the P-CSCF's Application Level Gateway (ALG) has the task to deal with NATed users (proxy, holds pinhole open, all communication goes through the P-CSCF). Last but not least, the probably biggest advantage of IMS is the easy way to deploy new services, which is very expensive in a P2P system, as a P2P system is usually designed directly on the use case (e.g. file sharing).

As a conclusion, we see that IMS is a nice technology, as long as it does not deal with media. This can be complemented by a P2P network, which is solely responsible for media distribution, but can also serve as alternative service provision platform to IMS services (e.g. community services, fall-back solutions, etc.)

# 6 Migration frame

## 6.1 Functionality Groups

The design of a migration frame for P2P services in NGN networks has been driven by the concept of a gradual integration of the two technologies in the context of the identification of an optimum point between the two planes. The process of such integration involves the replacement of certain functionality in the one plane with mechanisms provided by the operation of the other.

The overall target is the enhancement of IMS controlled media related services using the power offered by P2P networks and techniques. The main focus is on distribution of live and on-demand media content without excluding, however, traditional file sharing.

The starting point of this process involves the identification of the various functionalities that need to be present in the final assembly. There are four major categories that group together such functional aspects:

- User authentication/authorization and content security
- Publication and discovery of content
- Session establishment and maintenance
- Content Transfer

For each one of these categories a solution can be provided by using mechanisms provided by either technology. Such mechanisms may not be identically similar between the two technologies and the actual focus may vary. The following table presents for each category the candidate solution from each plane:

| | SIP/IMS Plane | P2P Plane |
|---|---|---|
| Authentication/ Authorization/ Content Security | User Registration, Accounting, User Profiles | Anonymity, password/key protected/encrypted files |
| Content Publication/ Discovery | SIP Presence, Contacts List | WEB Queries, DHT, Torrents |
| Session Establishment/ Maintenance | SIP INVITE | DHT, Centrally distributed list of peers |
| Content Transfer | RTP | P2P links, distribution of file pieces |

The sequence in the process of integrating mechanisms from the two planes along with an initial estimation of the possibility of using in the final assembly a mechanism of either plane is depicted in the figure below. The width of each

triangle at a specific functionality level indicates the possibility of deploying the corresponding plane's procedures in the leading role. Procedures relating to content transfer are based on the P2P side while signaling and control transactions are based on the IMS side.

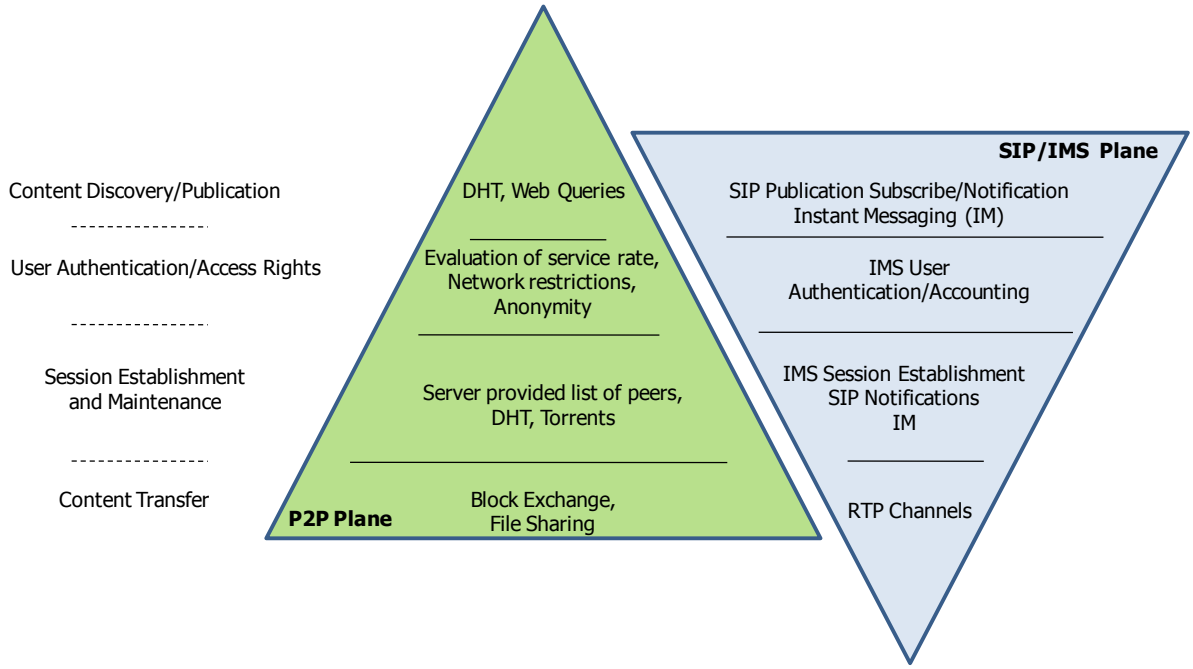


**Figure 1: P2P-IMS Integration Roadmap and Approach**

## 6.1 Migration Roadmap

### 6.1.1 Content Publication/Discovery and Session Establishment

In traditional P2P networks content is offered in forms of files. Each file is published on a central server against which certain queries, mainly based on the file name or keywords included in the filename, can be executed. Queries can result in lists of offered items. In case a list item is selected certain information based on hashed description text or pieces of the file is acquired by the client software along with a list of potential providers of the offered content. Thereafter, requests can be sent for locating and acquiring certain pieces of the file among the connected peers.

In IMS, connections are established between users that have knowledge of one another by means of a SIP-URI. The SIP-URI is communicated using non-IMS methods. Modifications in the status (mainly availability) of SIP-URI can be monitored using the services offered by the SIP Presence package.

In IMS systems, contrary to the P2P networks, there is knowledge of the entities to whom one can connect but the content (voice or video) transferred over this connections normally is not known in advance except for cases where invitations to SIP URI result in acquisition of media content (IMS based IPTV).

It is normally formed throughout the session since in most cases it is audio and/or video that is captured during the session.

In P2P networks the content is well known in advance or at least it is known before the data connections are established. The actual sources from where the content (entirely or in pieces) will be retrieved are made known throughout the operation of the P2P methodology. In many cases the bootstrapping overlay may be totally different from the overlay in the last phase of data transfer.

Aiming at using the IMS infrastructure as control plane in Vital++, the emerged concept with respect to content publication and discovery (content indexing) was to use a server side entity that communicates using SIP. The operation of such an entity is two-fold:

- It is notified of offered content under certain descriptions that can be used for searching
- It makes available in terms of lists with complete description the published items when certain search criteria are presented by other users

In this case the SIP-URI through which indexing information can be acquired remains valid inside the IMS infrastructure as long as it aids publication and discovery of media items according to a specific policy.

In essence, the P2P paradigm with respect to content discovery remains the same. However, the operation is provided by a node that is certified to offer such functionality and there can be the respective accounting that exists in IMS networks.

The protocol that is used to offer the envisaged indexing functionality is accommodated in SIP Instant Messages (IM).

Beyond that, the same entity is responsible for providing the overlay synthesis to users that are willing to acquire a specific media item. Modifications to the overlay syntheses are also communicated to previously bootstrapped nodes. Since such an entity is operating at the network side where network topology information can be available, the bootstrapping of new peers can be based on the processing of such information. Thus, the Overlay Management Subsystem that is envisaged can provide more optimal initialisation of the overlays aiding in better service experience from the very early moments of content acquisition.

### 6.1.2 User Authorisation, Content Security

Security issues are complementary to the indexing problems. P2P systems normally do not pose any limitations in content acquisition apart from adaptations of the experienced service rate depending on certain behaviour criteria that relate to volume of shared data or to uploading capacity. Files that are acquired from P2P interactions may be encrypted with secret keys that are

not provided by the P2P network but this remains out of the scope of the serving network.

On the other hand all the transactions in an IMS network can be restricted to those entities that have a valid account which is used to verify all of the transactions with the offered services. This means that there are means to fully control who has access to what and also maintain logs and charge for any service transactions.

Taking into account the fact that IMS procedures are inherently offering a full framework for communications among authenticated and authorised entities as well as clear identification of the users in terms of their stored subscription profiles, two additional entities are designed to cater for security needs.

The Content Protection (CP) Subsystem gives the possibility to users to publish media items under certain criteria such permissions and availability of the content. Additionally users can also associate security keys with the published content so that media are provided encrypted. In this way potential users of the published media items have to obtain the relevant keys from the CP Subsystem. Such an action binds the user identity with its approval on the fair use of the acquired content.

### 6.1.3 User Authentication

Beyond content security the project has dealt significantly with the fact that all transactions among users, starting from simple messaging and ranging up to more complex communication schemes, should allow for the verification of the authenticity of the message originator. This is not possible in regular P2P systems where identification cannot be extended beyond network addresses or simple user accounts that cannot not by any means be reliably associated with physical entities. In IMS the fact that SIP-URIs are bound to specific user accounts and profiles with which billing information can be also associated gives the opportunity to enable a digital certificate based identification of users. This can be done in both types of communications, either those passing through the IMS or those based on point to point transactions. In any case messages conveyed among users can be digitally signed and verified so that no anonymity is experienced or claimed.

### 6.1.4 Content Delivery/Distribution

Typically in an IMS session video and audio are captured and transmitted in real time, whereas in P2P sessions the content is aggregated in the form of media files where playback can start according to the user's preferences. In the hybrid solution provided by Vital++, content is distributed following a specific timeline to address and cope with the needs of live-streaming distribution of media. This, however, is based on sharing of blocks of media data among the peers of an overlay. Peers maintain the status of their

neighbours regarding the availability of data blocks and decisions are taken based to certain criteria for the next data transmission or request. Data blocks, however, are not fixed due to the time evolution of the content that is reflected in the maintenance of a sliding window of timely ordered blocks in every peer.

In this essence, the P2P methodology regarding data sharing is maintained in the combined approach. However, media information is characterised by the feature of live content as this is met in IMS sessions.

## 6.2 Functional Groups Integration Principles

Combining techniques and mechanisms of two different planes (P2P and IMS) requires modifications and adaptations on existing methods so that proper integration can be achieved. Each of the functionality groups should be designed in such a way that although it is operating according to its design principles, it can be used to provide the required input to other functionality groups.

The information flow among groups as well as the processing and usage of it inside each group is dictated by the following principles:

- All users can publish whatever media content they wish, on condition that this is not done anonymously
- Publication requires definition of criteria that define the eligible users
- Criteria might contain the availability during a period of time, pricing information, additional indications regarding the definition of the fair use of the content and even criteria with respect listing of the specific item in a query result to any other user
- Publication of an item makes the publisher responsible for the way the rights of the offered item have been managed (so that cases of improper use of the content are detected)
- Once publication has been submitted, the user becomes source of the offered item with respect to distribution overlays that this user may be involved thereafter
- Content can be encrypted by the user once the relevant material is generated and maintained in the system so that it can be acquired by authorised users. Encrypted content may be "super-distributed" throughout a content overlay.
- Publication should be also accompanied by the provision of indexing information that can be exploited during query processing for the discovery of offered media items
- Once a user has located an interesting media item he has to be authorised for accessing it
- After authorisation the user can receive a list of peers with whom he may connect in the context of the operation of the distribution overlay

- After joining an overlay a user becomes content source as well and should operate according to the distribution mechanisms of the overlay
- The user has to generate a digital certificate that has to be signed by the system
- In order to ensure message authenticity the user has to digitally sign all the messages he sends directly or indirectly to other users by use of the generated certificate
- Media are transmitter in the form of RTP packets. These should be placed inside P2P exchanged blocks and circulated in the overlay
- Upon reception of a P2P block the RTP packets should be extracted and forwarded to the playback components
- Encryption is applied at the RTP level by use of a key that has been generated by the publisher during publication of the item

All these principles indicate transactions among functionality groups by means of exchanged information.

# 7 Impact of P2P-NGN Integration

## 7.1 User Side

### 7.1.1 Modifications of Existing Components

Since the integration of the two technologies involves adoption of techniques met normally in one of the two, the remaining components should be adapted so that there is proper cooperation among all the elements of the assembly.

There is need for removing all the control mechanisms from the P2P components and replace these with mechanism that provide information coming from the control procedures carried out by the IMS components. Thus, the P2P elements should not perform any search and publication or other DHT based mechanisms for locating content that might be of the user's interest. Evolution of the overlay and modifications in the neighbours' peer list can be enabled in the context of the P2P operation so as to allow for more optimal decisions using the self-adaptability feature that can be embedded into the P2P algorithms. However, there is need for supporting modifications of the overlay to be injected into the P2P component, mainly regarding the removal or addition of certain peers. In this way, NGN based operations are used to bootstrap the peers for entering initially an overlay with more optimal conditions according to the knowledge of the network topology that may be available in NGN and there is always the possibility for the system to inform the overlays of arrivals or removals.

As far as media exchange is concerned, traditional playback operates on top of point to point circulation of RTP packets is adapted to work above a different transport mechanism provided by the P2P components. For this purpose special transport adapters are implemented so that playback modules do not perceive any change in the transmission or reception of RTP packets.

Additionally, session initiation and negotiation is not handled by SIP Invite dialogs. The transport settings (addresses and port numbers) are resolved by new components and used in the initialisation of the transport layer that is based on P2P procedures. The playback or media transmission engine is initialised with the new transport layer.

### 7.1.2 Introduction of Additional Components

User authentication, authorisation and content security procedures as well as content publication and discovery mechanisms have been defined in the context of the project so as to address the certain security and content management needs that have been imposed by the integrated approach. Therefore, additional components have been introduced in the client architecture.

The user authentication procedures require a component to handle the generation of the user certificate as well as all the signing and verification actions that are required. The new concepts become necessary since the NGN/P2P operation requires the communication among physical entities for which there was not any former relationship that normally in an NGN environment is expressed by the existence and maintenance of a contact list in the client software.

Publication and discovery of content involves both indexing and security aspects. Special components are designed and introduced in the client architecture that interfaces with the Content Indexing and Content Security subsystems. These cater for the user needs regarding publication of the content under specific indexing and security criteria. They also provide means for locating content, resolving access rights and authorising the user to retrieve certain media content. Finally, they allow the client software to receive the information for joining P2P overlays.

### 7.1.3 Architecture and Design Aspects

The realization of the UA according to the principles and roadmap presented above has to be based on a modular design. In this design functionality is grouped into modules. Each module depends on the services provided by other modules. Since there are more than one candidate modules for the provision of the required services, the interfaces among modules have to be designed in an abstract way. In this way the actual combination of modules can be done during the compilation of the runtime image of the UA.

The current approach is based on the realization of a UA by use of the Java language. The overall architecture of the UA is presented in the following figure.

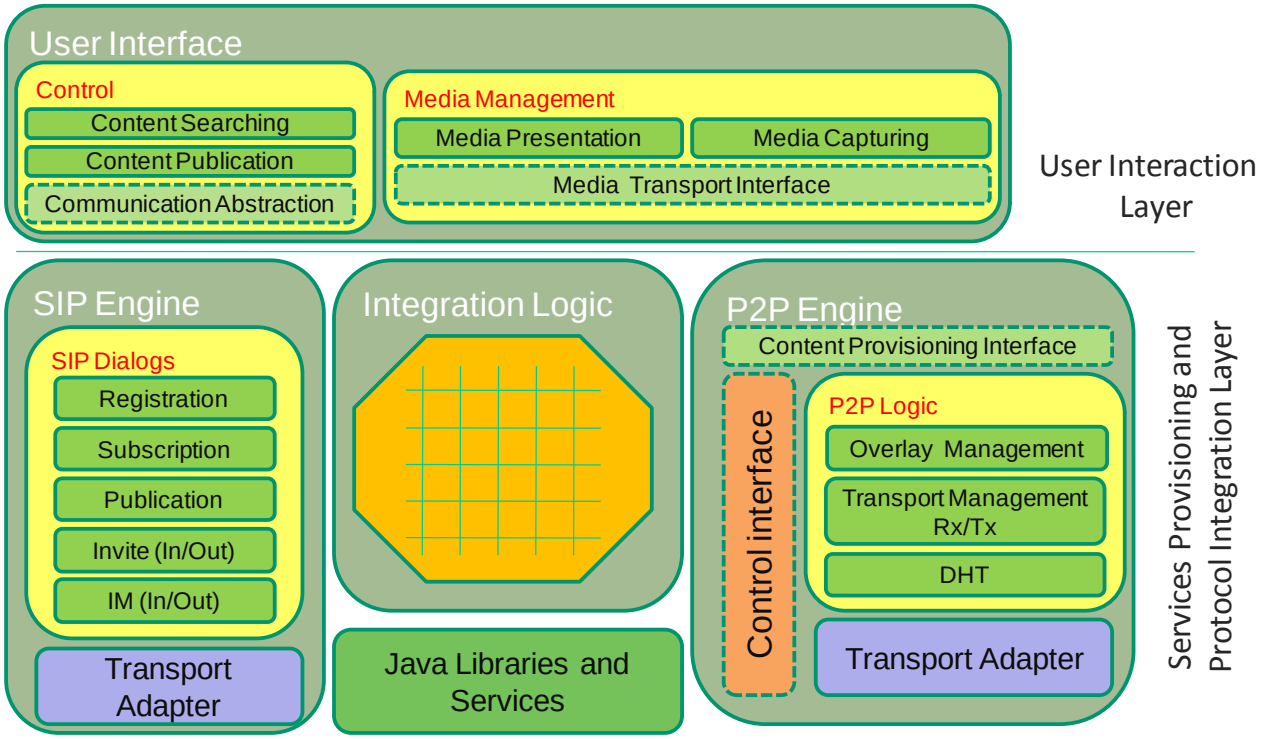


**Figure 2: Client Architecture**

The architecture of the client identifies three layers:

**User Interaction Layer**

It is the part of the client that interacts with the user. It provides all media playback and capturing capabilities as well as means for aiding the discovery and publication of content. This layer operates in a transport and communication agnostic manner. It produces and consumes both control information and media content. Control data are generated and processed by GUI elements that allow the user to navigate the acquired information. The control information that is produced identifies either criteria for content searching/publishing or content selection for acquisition and licensing through the underlying layers procedures. Media management contains all the required mechanisms for media representation or capturing by use of the available JMF libraries. Control on the Java Media Framework (JMF) components is restricted to configuration regarding media playback or capturing leaving transport layer dependencies to be handled by the underlying layers according to UA configuration.

**Services Provisioning and Protocol Integration layer:**

This layer contains one SIP engine and one P2P engine. The SIP engine is built as a library that allows for the establishment of a number of SIP dialogs. The dialog objects can be configured to provide the content that is exchanged in their lifetime so that it can be processed in other application modules for the provision of a specific service.

The P2P engine is built with a number of interfaces that can allow modification on the binding of these interfaces to specific objects according to the UA configuration. There is a number of Java interfaces defined that allow different classes to be instantiated and configured as the providers of specific services to the P2P engine. For example, the initial overlay synthesis can be extracted from a SIP IM and forwarded as a list of IP Addresses to the P2P engine or it can be gradually fed into the engine following a number of successful SIP Session negotiations with the list of the peers identified in the IM. Additionally the P2P engine provides a content exchange interface through which media content can be transmitted to the network or retrieved and forwarded to the media handling modules. In another instantiation the content exchanged at this interface might be blocks of a local file (Figure 3).

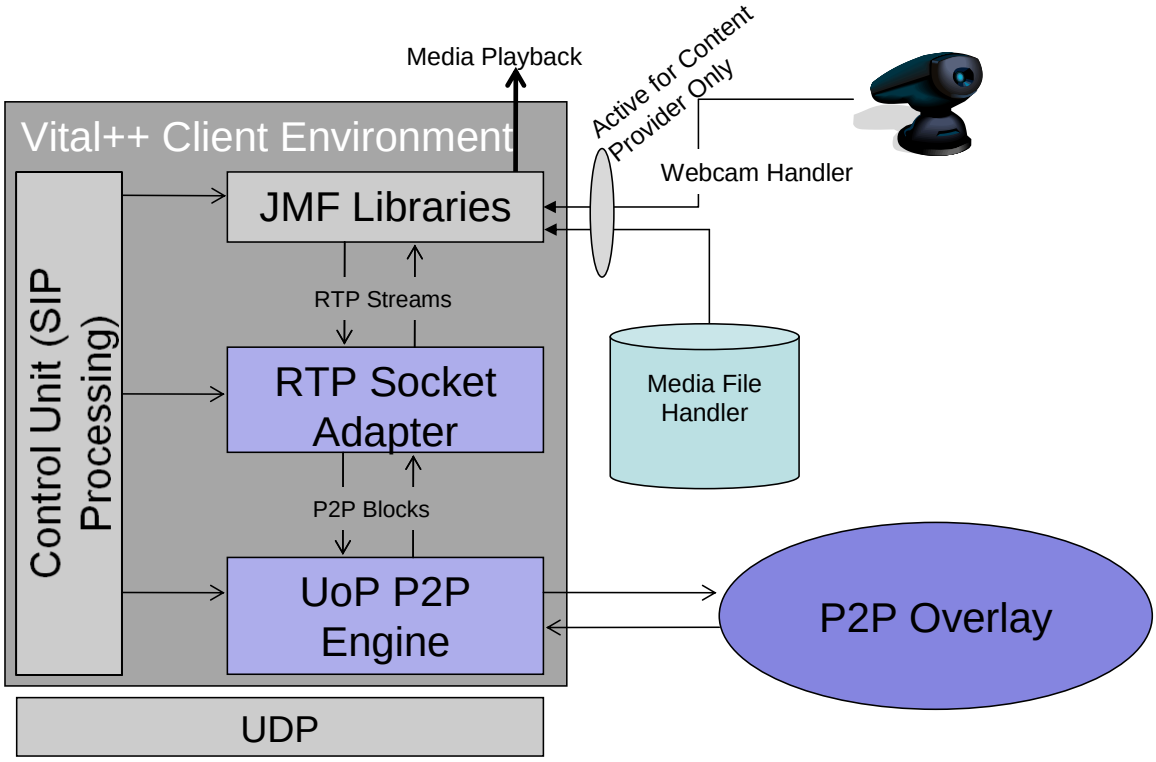


**Figure 3: P2P Engine Media Exchange Interface and Configuration**

Beyond the two engines, the capabilities of which are subject to integration according to the UA configuration, the Integration Logic block is the main element that binds together the rest of the modules. The binding materializes the actual combination of functionality aspects. Inside this unit specific integration objects are instantiated that make use of the services that can be provided by the other modules. The role of these integration objects is to map the events and messages generated during runtime by one module on the appropriate messages and events of another module. For example content publication and discovery may be mapped on SIP Presence (Publication/Subscription/Notification) events and dialogs or it can be handled using a custom protocol carried inside SIP Instant Messages (IM). In case DHT

is available and content publication/discovery has been bound to DHT procedures, the same events could have been mapped on specific DHT transactions.

There is also the possibility to bind a module on existing modules and services provided by the Java standard and/or extended runtime environment. For example in the instantiation of a pure SIP/IMS client the Media Management is bound onto standard Java UDP protocol handlers available in the JMF.

This layer includes also the Java and JMF objects that are instantiated as part of the integration procedure.

## 7.2 Network Side

In this section, we will describe the network side of the impact of the P2P-NGN integration. This basically means the impact on the IMS. As all IMS located functionalities of the Vital++ architecture have been designed to fit in a SIP application server, it was neither wanted nor necessary to modify existing components in the IMS.

### 7.2.1 Introduction of Additional Components

The only new component in terms of NGN components is the Vital++ application server (AS). In this AS, all functional blocks of the introduced sub-architectures are realized. The Vital++ AS can be deployed in a single node or distributed over multiple nodes. It is also possible to deploy only wanted sub-architectures, e.g. to omit the P2P-Authentication sub-architecture if no P2P authentication shall be supported. The following illustration depicts the relation of the single sub-architectures in a single AS and to the IMS environment.

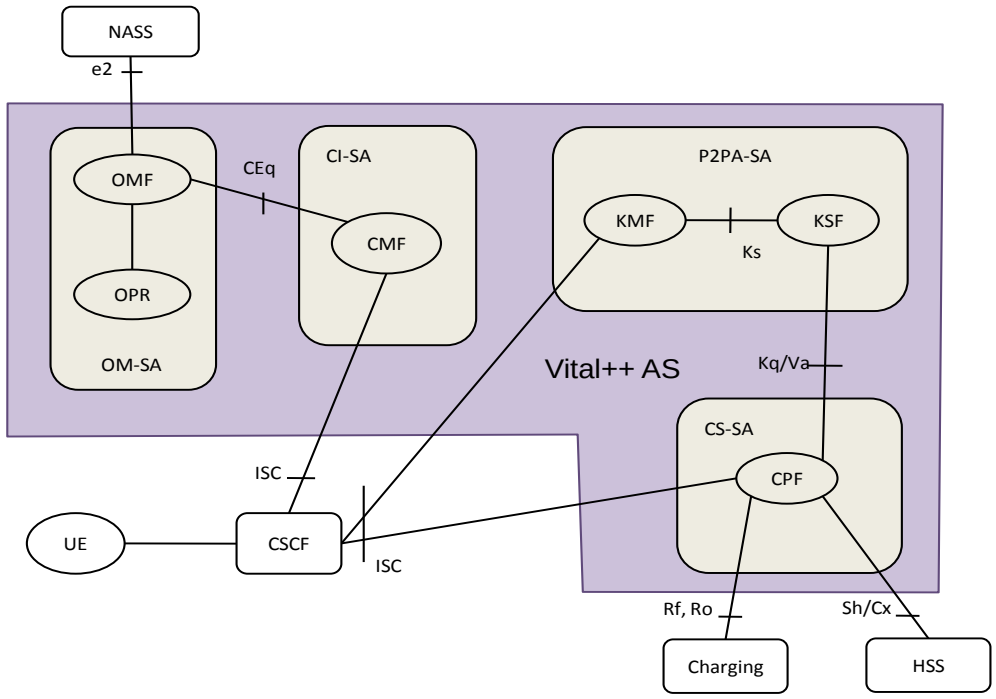


**Figure 4: Sub-Architecture oriented Structure of the Vital++ AS**

All sub-architectures communicate with the client user entity (UE) via the call/session control function (CSCF) of the IMS core via the ISc interface. This is realized according to the 3GPP standards using the session initiation protocol (SIP)[1][2]. Thus, the new features can all be utilized by the client without the deployment of new network protocols. The reason is that SIP is extensible in terms of protocol elements and transactions.

The Vital++ AS can access a network attachment sub-system (NASS) via the DIAMETER based e2 interface to retrieve information about the connectivity of a user, i.e. its upload and download bandwidth in order to build more efficient overlay networks. Also, the main IMS database, the home subscriber server (HSS) can be accessed to gain more information about the user. In order to produce call detail records for either online (prepaid) or offline (billed) charging, the AS can access IMS charging functions via the Rf and Ro interfaces, based on DIAMETER.

[1] 3GPP, TS 23.228: "3rd GPP; Technical Specification Group Services and System Aspects; IP Multimedia (IM) Subsystem - Stage 2"

[2] TS 24.228: "3rd GPP; Technical Specification Group Core Network; Signalling flows for the IP multimedia call control based on SIP and SDP".

### 7.2.2 Possible standardisation

As SIP is intended to be extended also in terms of new specifications, arising from IETF, 3GPP, ETSI TISPAN, or ITU-T[3] standardisation efforts, standardisation appears to be possible for the way how information is transported between the entities for the different procedures in the Vital++ architecture. These include:

- Content indexing
  - Content publication
  - Content search/lookup
- Overlay construction
  - Overlay search
  - Neighbourhood announcement
  - Overlay updates
- P2P Authentication
  - Certificate exchange
  - Message signature
- Content Protection (DRM over SIP)
  - Licence search
  - Licence shipment
  - Licence updates

## 7.3 Performance Improvement

In this section we will analyze the benefits and the improvements in the performance of the content distribution services for the integration between NGN and P2P architectures.

The major improvements in the performance of these services comes from the fact that through NGN mechanisms we can exploit information correlated with the structure of the network in which the proposed services operate. Additionally the entrance of a user through NGN components that are dedicated to the accomplishment of such an objective constitutes a fast and reliable mechanism for the discovery of the peers and servers that will be used for data exchange.

As far as it concern the P2P part it complements the features that NGN offers by providing scalable and self-organized solutions towards the content distribution graph management by exploiting the information that NGN offer. This task is also enhanced by measurements and decisions that peers can do dynamically and locally. Finally network and storage resources of the

[3] International Telecommunication Union, Standardization (ITU-T), http://www.itu.int/publications/sector.aspx?lang=en&sector=2

participating peers are combined with those that NGN management systems offer. So the integration of the two worlds offers an architecture that is able to exploit and organize the total amount of resources that exist in a network and its peripheral components as peers and servers.

More specifically the major technical objectives which the cooperation between the NGN and peer to peer is able to accomplish are:

- The fast insertion of a user to the system.
- The minimization of the traffic that content distribution services introduce in the underlying network.
- The minimization of the latency for the diffusion of the content to the participating peers.
- The maximization of the exploitation of resources of the participating peers.
- The stable and uninterrupted delivery of the multimedia streams.
- The minimization of the bandwidth resources that servers contribute and as a consequence the minimization of the cost of ownership that content distribution services have.

In the rest of this section we briefly present the concepts and the mechanisms that are able to achieve the aforementioned objectives while in the D3.1 and D4.2 we analyze these mechanisms in detail.

The content index servers except the directory service that they offer they are capable to manage information that is relevant with the set of peers that participate every moment in each object distribution. Through this database they can act as a peer discovery mechanism for every peer that enters the system and "suggest" to it other peers that are in the same network region and/or in the same autonomous system. This mechanism not only speeds up the insertions of a peer in the content diffusion graph but also adds intelligence in the initial neighbour discovery of each peer that enters the system.

Information that is relevant with the ISP and/or service provider that each peer has is offered by NGN relevant mechanisms and so peers are able to organize distributed a content diffusion overlay that minimizes the traffic that the content distribution introduces to the underlying network. This process is done dynamically by an overlay management algorithm that runs periodically in every peer while information relevant with this objective is offered through NGN mechanisms.

According to the aforementioned mechanism, participating peers are able to achieve fast diffusion of the content by selecting network paths that have low latency. This selection is also done from participating peers while NGN mechanism are capable to select for the peers application servers that are close to them.

The various peers that participate in object distributions are devices that have heterogeneous upload bandwidth capabilities. In such kind of environments

there is a need for the development of a graph structure that is able to maximize the resource utilization of the participating peers. Additionally there is a need for a dynamic graph adaptation to them and through the use of autonomic content diffusion P2P block schedulers the distribution of the data according to the bandwidth capabilities of the participating peers.

The application servers are able to offer bandwidth resources and ensure the stable and on time delivery of the multimedia streams. With this component and the development of a system that is able to monitor the resources of the peers we are in position to ensure through NGN mechanisms the uninterrupted stream delivery.

Finally and more important, by the use of the network and storage resources of the participating peers NGN are capable to deliver these kind of services with very low cost. In more detail, application serves contribute resources only in case where participating peers in an object distribution are not able to deliver the stream completely. Additionally the storage of the former acts as a network cache without introducing additional overhead and saves equipment to the service and/or content provider.

# 8 Integration Outcome

## 8.1 API Offerings

The integration of the Vital++ clients is based on a number of components that have been designed and implemented in the context of the Vital++ platform realisation. Each of these components caters for the needs of the Vital++ clients to interact with the server-side sub-architectures. In essence, every component can be fed with information or content and produce output that is compatible with the platform or on the other hand output that is usable in the context of the operation of the client with respect to content management.

All of these components are provided as Java library archives that can be easily integrated in a Java application. For each one there is a specific API through which the provided functionality can be invoked and used for making the application assembly compliant with the Vital++ platform services. The offered functionality ranges from processing of digital certificates or publication keys to data exchange through a P2P overlay. More specifically the offerings of the client components in terms of available API and functionality are summarised below:

- P2PA Component:
  - Generation of client certificate
  - Verification of peers and AS certificates
  - Message digital signing
  - Verification of signatures
- Content Protection Component:
  - Generation of licensing requests and responses
  - Generation of encryption keys for published items
  - Generation of messages carrying publication rules
  - Decryption of encryption-protected content
- Content Indexing Library:
  - Generation of CI function related (publish, query, select, etc) messages
  - Processing of incoming CI messages
  - Association of call-back objects with published items, selected items, peer lists
- SRTP plug-in
  - It allows outgoing RTP streams to be encrypted and incoming ones to be decrypted by use of secret keys that cater for content licensing
- P2P Engine

- Configurable with respect to overlay neighbourhood
- Push and pop capabilities of indexed content blocks
- Overlay updates

All these components are integrated in the Vital++ clients in the way that is dictated by the realisation of the envisaged use cases. Further usage paradigms and associations are not excluded or limited.

## 8.2 Platform Offerings

The Vital++ platform provides a set of services realised and offered by Application Server elements that are described in detail in D3.1. These services have been designed in a way that supports the realisation of a system allowing for effective and adequate content distribution with proper control of the consumption of multimedia material with respect to digital rights, accounting, licensing and user authentication. Although, the Vital++ AS is used in a very specific way in the context of the project's use cases, additional applications may be envisaged and created on the basis of the availability of the indexing, authentication, overlay management and licensing capabilities offered.

# 9 Conclusions

In this document we have presented aspects and approaches on the basis of which the actual design and implementation work has been carried out. The outcome of this process has been based on the separation of functionality into functional groups. Each of these groups caters for different needs and operations. However, the integration of these procedures leads to the provision of the envisaged platform and services.

Technical details on the different aspect presented above can be found in other technical deliverables:

- Peer to peer authentication, Content Indexing, Content Protection and Overlay Management are described in D3.1
- Authentication & Accounting is defined in D4.1
- Applications built on top of the Vital++ platform and their relation with Content protection are described in D4.2

**- End of document -**