# D4.1.2

# Consolidated Network Service Provisioning Concept

# Version 1.0


## WP 4.1 Mobile Network Architecture, Design & Implementation

## Dissemination Level: Public

Lead Editor: Nuno Inácio, IT-Aveiro

21/11/2005

Status: Final

**SIXTH FRAMEWORK PROGRAMME**

**PRIORITY IST-2002-2.3.1.18**

*Grid for complex problem solving*

*Proposal/Contract no.: 004293*

**License**

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

**1. Definitions**

a. **"Collective Work"** means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this License.
b. **"Derivative Work"** means a work based upon the Work or upon the Work and other pre-existing works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work will not be considered a Derivative Work for the purpose of this License. For the avoidance of doubt, where the Work is a musical composition or sound recording, the synchronization of the Work in timed-relation with a moving image ("synching") will be considered a Derivative Work for the purpose of this License.
c. **"Licensor"** means the individual or entity that offers the Work under the terms of this License.
d. **"Original Author"** means the individual or entity who created the Work.
e. **"Work"** means the copyrightable work of authorship offered under the terms of this License.
f. **"You"** means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received express permission from the Licensor to exercise rights under this License despite a previous violation.

**2. Fair Use Rights.** Nothing in this license is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

**3. License Grant.** Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

a. to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;

b. to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works;

The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats, but otherwise you have no rights to make Derivative Works. All rights not expressly granted by Licensor are hereby reserved, including but not limited to the rights set forth in Sections 4(d) and 4(e).

**4. Restrictions.**The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

a. You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy or phonorecord of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this License Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this License. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any reference to such Licensor or the Original Author, as requested.
b. You may not exercise any of the rights granted to You in Section 3 above in any manner that is primarily intended for or directed toward commercial advantage or private monetary compensation. The exchange of the Work for other copyrighted works by means of digital file-sharing or otherwise shall not be considered to be intended for or directed toward commercial advantage or private monetary compensation, provided there is no payment of any monetary compensation in connection with the exchange of copyrighted works.
c. If you distribute, publicly display, publicly perform, or publicly digitally perform the Work, You must keep intact all copyright notices for the Work and give the Original Author credit reasonable to the medium or means You are utilizing by conveying the name (or pseudonym if applicable) of the Original Author if supplied; the title of the Work if supplied; and to the extent reasonably practicable, the Uniform Resource Identifier, if any, that Licensor specifies to be associated with the Work, unless such URI does not refer to the copyright notice or licensing information for the Work. Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.
d. For the avoidance of doubt, where the Work is a musical composition:
    i. **Performance Royalties Under Blanket Licenses**. Licensor reserves the exclusive right to collect, whether individually or via a performance rights society (e.g. ASCAP, BMI, SESAC), royalties for the public performance or public digital

performance (e.g. webcast) of the Work if that performance is primarily intended for or directed toward commercial advantage or private monetary compensation.

ii. **Mechanical Rights and Statutory Royalties**. Licensor reserves the exclusive right to collect, whether individually or via a music rights agency or designated agent (e.g. Harry Fox Agency), royalties for any phonorecord You create from the Work ("cover version") and distribute, subject to the compulsory license created by 17 USC Section 115 of the US Copyright Act (or the equivalent in other jurisdictions), if Your distribution of such cover version is primarily intended for or directed toward commercial advantage or private monetary compensation.

e. **Webcasting Rights and Statutory Royalties.** For the avoidance of doubt, where the Work is a sound recording, Licensor reserves the exclusive right to collect, whether individually or via a performance-rights society (e.g. SoundExchange), royalties for the public digital performance (e.g. webcast) of the Work, subject to the compulsory license created by 17 USC Section 114 of the US Copyright Act (or the equivalent in other jurisdictions), if Your public digital performance is primarily intended for or directed toward commercial advantage or private monetary compensation.

**5. Representations, Warranties and Disclaimer**

UNLESS OTHERWISE MUTUALLY AGREED BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE WORK, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

**6. Limitation on Liability.** EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

**7. Termination**

a. This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Collective Works from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.

b. Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted

under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

**8. Miscellaneous**

a. Each time You distribute or publicly digitally perform the Work or a Collective Work, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.
b. If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.
c. No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.
d. This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Licensor and You.

**Context**

| | |
|---|---|
| **Activity 4** | Detailed Architecture, Design & Implementation |
| **WP 4.1** | Mobile Network Architecture, Design & Implementation |
| **Dependencies** | Uses input from D3.1.1<br>Based on work from WP3.1, WP4.2, W4.3, WP4.4<br>Integration work on WP5.1 may depend on this deliverable |

| **Contributors** | **Reviewers** |
|---|---|
| Ruth del Campo (UStutt-RUS)<br>Patrick Mandic (UStutt-RUS)<br>Nuno Inácio (IT Aveiro)<br>Rui L. Aguiar (IT Aveiro)<br>Susana Sargento (IT Aveiro)<br>Dirk Haage (UPM)<br>Vicente Olmedo (UPM)<br>Víctor A. Villagrá (UPM)<br>Jose Ignacio Moreno Novella (UPM)<br>Isabel Alonso (TID)<br>Arantxa Toro (TID) | Review by partners external to 4.1:<br>Per-Oddvar Osland (Telenor)<br>Antonis Litke (NTUA) |

**Approved by: QM**

| **Version** | **Date** | **Authors** | **Sections Affected** |
|---|---|---|---|
| 0.1 | 14/4/05 | TID | All (Table of Contents) |
| 0.2 | 30/6/05 | All | All |
| 0.3 | 24/9/05 | All | Updates to most sections |
| 0.4 | 3/11/05 | Nuno Inácio, Patrick Mandic | Added Service Provisioning Architecture and Executive Summary sections; ready for reviewing |

| | | | |
|---|---|---|---|
| 0.5 | 17/11/05 | All | All sections updated according to review by Akogrimo partners |
| 1.0 | 21/11/05 | Nuno Inácio | Final version |

# Executive Summary

This document describes the different points of interaction between the network infrastructure and the Grid running on top of it. The architecture of this network infrastructure, its requirements, and components were detailed in D4.1.1. The current document takes this architecture as a starting point and emphasizes the symbiosis between the network infrastructure and the Grid from the point of view of the network side while tackling other innovative aspects not necessarily inherent to the classical network architecture approach, such as the handling of "user location".

First, the requirements imposed by this interaction between Network and Grid are analyzed, covering functional as well as non-functional requirements. Starting from this base, the reasoning of the services to be granted to other layers -such as Mobility or QoS- follows. These Network services are virtualized and seen - from the point of view of the Grid - as any other resources such as storage or computational power. An example could be capability of the Grid to schedule a QoS reservation - e.g. a certain bandwidth, assure minimum delay or jitter... - for an allocated task that requires it.

This document describes the necessary background, tools, techniques and corresponding protocols to be used in order to achieve such a challenging task and concludes with a more concrete description of the way network resources can be implemented as part of the whole network infrastructure architecture to render the Grid the most valuable service.

# Table of Contents

# List of Figures

# List of Tables

# Abbreviations

| | |
|---|---|
| **A4C** | Authentication, Authorization, Accounting, Auditing and Charging |
| **AA** | Authentication and Authorization |
| **AAA** | Authentication, Authorization and Accounting |
| **Akogrimo** | Access To Knowledge through the Grid in a Mobile World |
| **AN** | Access Network |
| **API** | Application Programming Interface |
| **COPS** | Common Open Policy Service Protocol |
| **CPU** | Central Processing Unit |
| **DiffServ** | Differentiated Services |
| **DoS** | Denial of Service |
| **DSCP** | Differentiated Service Code Point |
| **HA** | Home Agent |
| **HoA** | Home Address |
| **IETF** | Internet Engineering Task Force |
| **IntServ** | Integrated Services |
| **IP** | Internet Protocol |
| **IPSec** | IP Security Protocol |
| **IPv6** | Internet Protocol version 6 |
| **LAN** | Local Area Network |
| **LDAP** | Lightweight Directory Access Protocol |
| **MIPv6** | Mobile IPv6 |
| **MN** | Mobile Node |
| **MT** | Mobile Terminal |
| **PANA** | Protocol for carrying Authentication for Network Access |
| **PBNM** | Policy Based Network Management |
| **PBNMS** | Policy Based Network Management System |

| | |
|---|---|
| **PDA** | Personal Digital Assistant |
| **PGP** | Pretty Good Privacy |
| **QoS** | Quality of Service |
| **QoSB** | Quality of Service Broker |
| **RSVP** | Resource-Reservation Protocol |
| **RTP** | Real-Time Protocol |
| **RTSP** | Real Time Streaming Protocol |
| **SDP** | Service Discovery Protocol |
| **SIP** | Session Initiation Protocol |
| **SNMP** | Simple Network Management Protocol |
| **SOAP** | Simple Object Access Protocol |
| **SSL** | Secure Socket Layer |
| **TCP** | Transmission Control Protocol |
| **TLS** | Transport Layer Security |
| **UDP** | User Datagram Protocol |
| **UMTS** | Universal Mobile Telecommunications System |
| **URI** | Uniform Resource Identifier |
| **URL** | Uniform Resource Locator |
| **WLAN** | Wireless Local Area Network |
| **WS** | Web Service |

# 1. Introduction

The Akogrimo project aims to integrate a Next Generation Grid with a Next Generation Network, providing users with a secure, heterogeneous mobile environment with quality of service, supporting dynamic resource sharing and pervasive services.

This document describes the services that Akogrimo WP 4.1 Mobile Network Architecture, Design & Implementation will provide to Grid Infrastructure Services Layer and Grid Application Support Services Layer (henceforth referred to as "grid layers") as well as to the services and applications built upon the Akogrimo architecture.

D4.1.1 Consolidated Network Layer Architecture presents the network layer architecture and this document extends that work by focusing on grid layers requirements from WP4.1 and presenting the solutions for those requirements.

# 2. Network Service Provisioning

## 2.1. Overview

The following picture shows an overall view of Akogrimo architecture; it's split into functional layers (Mobile Internet, Network Middleware, Grid Infrastructure Layer, Generic Application Support Services Layer and Domain and Application Specific Services).

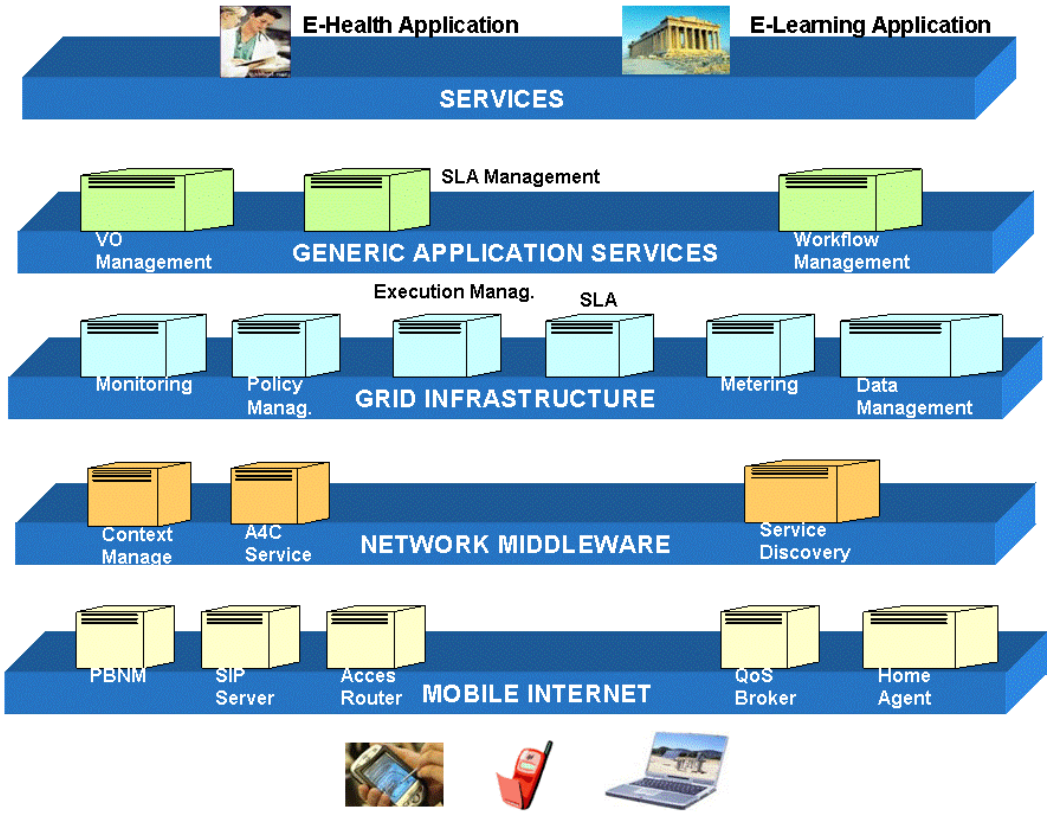


**Figure 1 Akogrimo Functional Layers**

In figure 1, the first layer is the Mobile Internet layer and its main functionality is the combination between Mobile IP and SIP [SIP] to enable mobility supporting approaches, security, network service provisioning and network resource management.

The second Layer is Network Middleware. The main functions of this layer are:

- AAA (Authentication Authorization, Accounting), which will be brought into the Akogrimo overall architecture,
- Context Management, which involves the gathering of raw context data from different context data sources across well-defined interfaces
- Service Discovery, which allows a service requestor to find an appropriate service provided by a service provider)

Third Layer is Grid Infrastructure Layer, which covers:

- Execution Management (is related problems of instantiating and managing tasks) ,

- Data Management (is related to data management in Grid systems and applications and, finally, on the interactions with other components of the Grid Infrastructure Services Layer),
- Monitoring (monitoring data represents an operational photograph of the system behaviour along the time axis. Such information turns to be fundamental to determine the origin of the problems or to tune different system components),
- SLA subsystem (offers to Akogrimo infrastructure the management of all aspects related to the fulfilment of a quality of service (QoS), that is conditions agreed between the Service Costumers (SC) and the Service Providers),
- Metering services (this component is responsible to keep track of usage of specific resources that are utilized within the execution phase, for instance, CPU-time, Bandwidth…)
- Policy management (is the component responsible for the handling of the policy that will be applied in the execution of the various jobs).

The following layer is Generic Application Services. The main functions which cover this layer are:

- VO management (providing capabilities to subscribe new participants (users, service providers, etc.) inside the VO, to register those participants enabling them to sign-in their presence in VO, to support publishing phase of services and to check the access rights for invoking services),
- SLA management (in order to establish the QoS between service provider and service customer).
- This layer must also provide functionalities individuated for developing the application software for several devices, enabling the interactions with Akogrimo VO.

Behind the application layer every entities is seen as service (in particular, Web service or WS-resource) and this layer enables applications to found their capabilities over provided services. Two applications/services that exploit the Mobile Grid technology are going to be developed in the Akogrimo project, the Heart Monitoring and Emergency Response (e-Health) and the Field Trip (e-Learning).

## 2.2. Functional Requirements of the Mobile Network layer

The main functional requirements in Mobile network layer are the following:

1. **Mobility management** is an essential part of mobile networks. Mobile users will be roaming across different access networks (the first project phase will not consider UMTS access) and the network must know, at any time, where a mobile terminal is, in order to maintain connectivity. If multiple network providers are present, handovers among them are also be possible (the first project phase will only consider single layer), assuming that they have an agreement. Additionally, the network must ensure the authentication of the mobile terminal, communication security, access to network services and communication with other network nodes.

   Related Mobility Akogrimo project will mainly involve different types of mobility such as terminal Mobility, Personal Mobility or Session Mobility. These types of mobility are detailed in Section 3.2.

2. Provide an integrated platform to **provide network services** to the higher grid layers. This includes a signalling framework to support all relevant user/network interactions, so from a practical point of view, this services provisioning will be supported by a SIP infrastructure.
3. Functions related to **Security**. IPsec [IPSEC] will provide a secure access to the core Akogrimo network by means of encrypted IP tunnels. The security subjects will be considered in the second phase of the project.
4. Functions related to **network resource management** and **quality of service** issues. These functions will control not only user requests to network services, but also handovers between different access networks. They will allow that a user will get the service he paid for, i.e. guaranteeing a set of parameters to users, such as bandwidth, packet delay, etc.

In order to show how these functionalities allow services execution, let's consider the e-Health scenario, the Heart Monitoring and Emergency Response service, for instance. There is a patient pertaining to a risk group with diabetes and hypertension. He is wearing a couple of medical sensors forming a local patient monitoring network. The patient is abroad on a business trip, and suddenly feels a pain and needs medical attention. He uses his mobile phone to call for assistance and transmits his cardiological data with the help of ECG equipment integrated into his phone. This point is related to Terminal Mobility because, the patient is abroad and he needs to access an external network to reach the e-Health service.

His data is received in an emergency control centre. There, a virtual emergency environment (VEE) is automatically constructed, in which all information needed for the optimum care of the patient is made available. This information is processed through an embedded processing algorithm and made available to all those involved in the subsequent rescue process.

An emergency operator joins the VEE, and the establishment of an audio link to the patient is initiated in the connected Voice over IP network. The functionality SIP session establishment allows this.

Another example would be, in an e-Learning scenario, a student who is performing a simulation over his PDA and wants to move the session to his laptop, because the images resolution is not too fine. So, in order to get this issue is necessary the SIP session transfer functionality.

## 2.3. Non-functional Requirements of the Mobile Network layer

Some non-functional characteristics required by the Akogrimo platform are the following:

1. **Scalability:** the system's ability to grow (in number of users, terminals, traffic volume etc) without causing undesired side effects.

   The overall Akogrimo network is designed to be as scalable as possible. A Core Network supports multiple Access Networks, where the network entities, that will be subject to more work load, are located, helping to distribute processing power through the various network elements.

   Also, SIP [SIP] technology used in Akogrimo can handle multiple simultaneous communication sessions. From a practical perspective, SIP's scalability means that many people can participate in spontaneous, media-rich and interactive activities at the same time; this applies to audio and video conferencing, application sharing and any other collaborative activity. On the other hand the Grid computing technology used in Akogrimo, as well, can be a cost effective way to resolve IT issues in the areas of data, computing and collaboration;

especially if they require enormous amounts of computing power, complex computer processing cycles or access to large data sources. So Grid technology scalability means large number of resources, many participants, and many program components.

2. **Flexibility**: the overall architecture should adapt itself quickly to technological changes.

   SIP's philosophy of keeping things simple and not implementing functionality in a manner specific to voice, text, data or video permits the easy extension of SIP to support new media types and services in existing IP networks. SIP can accommodate video teleconferencing, for example, as easily as it can accommodate voice conferencing - and this is the central reason for SIP's rapid acceptance as an industry standard.

   Other technology used in Akogrimo (Grid technology) is flexible enough, as well, to deal with many resource types.

3. **Modularity:** the overall system is composed by several components and can be easily maintained and/or modified. Akogrimo architecture is designed in a modular way, and it involves many components, as shown in figure 1 (A4C, PBNM, SIP Proxy, Access Router, Metering, SLA,…), thereby the overall architecture will be easily maintained.

4. **Security**: the overall system should be secure (for instance, in an e-Health scenario, one patient's record should not be available to unauthorized users under any circumstances).

   IPsec will provide a secure access to the core Akogrimo network by means of encrypted IP tunnels.

5. **Reliable**: the system should be reliable. For instance, in an e-Health scenario, one patient who is receiving help from a doctor, needs a reliable service, otherwise his life may even be at risk. Another instance, in an e-learning scenario (Field Trip), a student who is doing a simulation with his data wants a reliable service, as well.

6. **Availability**: This characteristic is very important, for instance in an e-Health scenario, when a patient feels ill and wants to call a doctor by phone, but the access network or the Akogrimo platform are unavailable. There are several access networks to the Akogrimo core network: a Wireless Access Network, a Mobile Access Network and an Internet Service Provider. So the availability of the overall architecture will firstly depend on the availability of resources in the access network, and also on the core network availability.

   High-availability solutions for VoIP/SIP networks address the need for users to be able to place and receive calls under peak-load call rates or during device maintenance or failure. In addition to lost productivity, voice-network downtime often results in lost revenue, customer dissatisfaction, and even a weakened market position. Various situations can take devices off line, ranging from planned downtime for maintenance to catastrophic failure.

   There are two key elements that contribute to availability in a VoIP/SIP network: capacity and redundancy. These concepts will now be explored as follows:

   - *Capacity*: is a measurement of the volume of traffic a network is engineered to handle. Voice networks are typically engineered to handle a target peak-load capacity, commonly measured in calls per second. Target peak-load capacities are specific to each business and industry, and are based on measured busy-hour call rates.
   - *Redundancy*: measures the extra capacity, to be used only in the event of an equipment failure that is placed in a network. When a primary node in a voice network is taken down for maintenance or failure, a redundant secondary device can take over the processing of the voice.

   Into the core network, the Grid architecture is related with resource allocation, information sharing, and high availability. Resource allocation ensures that all those that need or request

resources are getting what they need. Information sharing makes sure that the user's information and needed applications are available where and when it is needed.

7. **Performance**: some parameters that define this non-functional requirement are: End-to-End Delay, the Jitter, Packet Loss and Out-of-Order Packet Delivery.

   - ***End-to-End Delay***: It can be of 2 types: Delays due to processing and transmission of data and Network delay, which is the result of processing in end systems, packet processing in network devices and propagation delay between network nodes on the transmission path. It comprises a fixed and a variable part.

     - Fixed part depends on performance of the network nodes on the transmission path, the capacity of links between the nodes ,transmission delay and propagation delay.

     - Variable part is the time spent in the queues which depend on current network load. Queuing delay can be reduced by introduction of advanced scheduling mechanisms (Expidited Forwarding and priority queuing). IP packet delay can be reduced by sending shorter packets. Useful technique for voice delay reduction on WAN is link fragmentation and interleaving. Here a longer packet is fragmented into smaller packets and transmitted. In between those small packets, voice packets are sent.

   - ***Jitter***: Delay variation, also called jitter, obstructs the proper reconstruction of voice packets in their original sequential and periodical pattern. It is defined as difference in total end-to-end delay of 2 consecutive packets in the flow. Removing the jitter requires collecting packets and storing them long enough to allow the slowest packets to arrive in order to be played in the correct sequence. Solution is to employ a playout buffer at the receiver to absorb the jitter before outputting the audiostream. packets are buffered until their scheduled playout time arrives. Scheduling a later deadline increases the possibility of playing out more packets and results in lower loss rate, but at the cost of higher buffering delay.

     Some techniques for Jitter Absorption are:

     - Setting the same playout time for all the packets for entire session or for the duration of each session.

     - Adaptive adjusting of playout time during silence periods regarding to current network delays.

     - Constantly adapting the playout time for each packet. This requires the scaling of voice packets to maintain continued playout.

   - ***Packet Loss***: It basically happens when the IP packet does not arrive to the receiver in time. Loss may be single frame or a block of frames.

     Techniques used to fight the frame erasure:

     - Forward Error Correction (requires additional processing) depends on the rate and distribution of the losses.

     - Loss concealment ( replaces lost frames by playing the last successfully received frame) effective only at low loss rate of a single frame.

     High frame erasure and delays can lead to a longer period of corrupt voice. The speech quality perception by the listener is based on frame erasure levels that occur on the exit from the jitter buffer after the Forward Error Correction has been employed. To reduce levels of frame loss, Assured forwarding service helps to reduce network packet loss that occur because of full queues in network nodes.

- ***Out-of-Order Packet Delivery:*** Occurs in the complex topology where more than one path exists between the sender and the receiver. The receiving system, must rearrange received packets in the correct order to reconstruct the original speech signal.

  Techniques for out-of-order packet delivery It is also done by Jitter buffer whose functionality now became

  - Re-ordering of out of order packets (based on sequence number)
  - Elimination of Jitter

  In the Akogrimo project, Mobile IP and SIP protocols work together in order to get the Performance improvement. For instance, with Mobile IP is possible the Fast Handover avoiding the loss of packets during the handover process and consequent degrading of quality in applications that are making use of the network.

8. **Efficiency**: Akogrimo will focus on two protocols (Mobile IP and SIP) related Mobile Network Layer, in order to tackle the mobility issues in an efficient way. So, Akogrimo will use together Mobile IP and SIP in order to provide Terminal Mobility, User Mobility and Session Mobility.

# 3. Network Services

## 3.1. Overview

The Akogrimo network will provide a variety of network services. Some of those services are essential for the network's own use, such as signalling protocols that support its basic functioning, and, without which, all network operations would not be possible.

The task of integrating network and grids implies providing grids with some form of control of basic network functionality, therefore it is necessary for the network layer to provide grids with services that allow the grid to control part their functionality, even if partially.

This chapter describes the most relevant network services provided to grids, in light of grid requirements described in the Akogrimo scenarios.

## 3.2. Mobility

### 3.2.1. Taxonomy

Mobility is a node's capability to change its position regardless of whether this position is physical or virtual. Diverse technologies grant the possibility of movement in different fashions, providing different functionalities and solving different kinds of problems. As stated in D3.1.1 several different kinds of mobility will be supported:

- **Terminal Mobility:** The ability to move a terminal while maintaining access to services and applications. This requires mechanisms for fast handover and location management. In Akogrimo it will be achieved with the use of a terminal with Mobile IPv6 capabilities [MIPv6]. By using MIPv6 the network layer handles exclusively this movement while the rest of the layers, above and below, are unaware of it. Handovers are possible without on-going connections being disrupted or broken and without applications being aware of the change of location of the device. MIPv6 manages mobility with the device's IP address. That is why it supports mobility of devices, but not of users or sessions. SIP can also be used to provide device mobility, however this is not as transparent to other layers as it is with MIPv6, it is not so optimized and the handovers become very noticeable. This is the reason why the type of mobility provided by SIP is called nomadicity.
- **Personal Mobility:** enables the user to access to telecommunication services regardless of the terminal being used. Besides, it is the network ability to identify the user when he is moving. This ability relies on the use of a single personal identity. SIP protocol plays a very important role about personal mobility, in Akogrimo.
- **Session Mobility:** This type of mobility allows the user to transfer an on-going session from one device (source device) to another (target device). In Akogrimo this will be achieved with the SIP protocol.
- **Inter-domain Mobility:** This is a new dimension of mobility in which users/devices can use resources and be reached in foreign network administration domains. This is accomplished by making use of A4C services (cf. WP4.2 A4C) with the Diameter protocol. To this end, both domains must hold an agreement, provided that this exists the foreign A4C will take care of authenticating, authorizing, accounting, auditing and charging keeping in touch with the home A4C, much like the way 2G cellular phones roam in different networks with the major addition of being based in all-IP networks. An example of how this is useful in the Akogrimo scenario would be that the requirements of an on-going Grid workflow triggers the change

from a network provider to the other because of e.g. QoS or bandwidth requirements. This type of mobility is handled in WP4.2.

Mobility in this project is not about accessing a Grid core from an uncorrelated mobile network infrastructure – it is about Grids to be aware of the existence of an underlying network and vice versa. With this background and according to mobility, nodes may be described with the following characteristics:

**Mobility aware:** This means that relevant information about mobility can be understood and taken profit of. These nodes with supporting this kind of mobility, do not have to just be aware of their mobility themselves, but also understand the movement information related to others.

**Mobility unaware:** Information about mobility cannot be processed or understood.

**Static:** No movement or change of location is possible for these entities. However, this does not mean that they can not understand mobility information related to other nodes. Typically static resources are related to nodes for heavy computing, databases, File servers and so on.

**Mobile:** These entities can freely roam networks. The fact that a resource is mobile does not necessarily imply that it is aware of its mobility; mobility may be totally transparent to higher layers. However, as a general rule one would like to be mobility aware in order to take profit of it and try to palliate the drawbacks. Typically mobile resources are not just related to smaller computers such as PDAs or laptops but also can be people moving around and using different devices (which may be static by nature).

According to this we can classify nodes in four different groups:

| | |
|---|---|
| Static & Mobility Unaware | Mobile & Mobility Unaware |
| Static & Mobility Aware | Mobile & Mobility Aware |

**Table 1 Grid resources classification**

It can be seen that some nodes are totally mobility agnostic, they do not move or are not able to understand mobility information. An example of such a type of node could be a service offering a simple sum of two numbers. There is no need for this service to be mobile or be aware that the user may be moving. Other nodes are static but nevertheless mobility aware, and therefore are able to understand mobility information about peers. A node can be mobile, however the applications may not be aware of its mobility - MIPv6-based mobility would be a paradigm of this. At last, nodes can be mobile and mobility aware at the same time.

From the WP4.1 point of view, we typically consider SIP-based applications as mobility Aware whereas MIPv6-based applications are mobility unaware. However mobility awareness can be achieved by means of other components, like the Context Manager in the WP4.2. For instance, a node may transparently change from one network to another by making use of MIPv6, however the context will probably change. Context includes things like type of connection, bandwidth available.

### 3.2.2. Mobility services

The mechanisms provided in WP4.1 to support mobility are based in SIP and MIPv6. The type of mobility provided depends on the purpose of the node application that the node is supposed to handle. These technologies are not mutually excluding and can be used together to provide different kinds of mobility for the same entity.

**MIPv6:** In a totally transparent fashion to other layers, MIPv6 provides device mobility by allowing the point of attachment to the network to change seamlessly. Provided that mostly wireless networks are used, this allows fully physical movement. Applications running with MIPv6 as underlying network layer use a single address independently of the network in which the node is located. A node communicating with a mobile node with MIPv6 should also use MIPv6 to diminish the amount of overhead in the communication. From the point of view of WP4.1 when a mobile node changes its point of attachment to the network a mechanism will try to provide the new communication established with the same security level (typically IPsec), QoS characteristics accorded, and so forth, however this is transparent to other layers and handled by the network internally. The only way to learn about these changes would by means of the context manager in WP4.2.

**SIP:** Session and user mobility are possible with the SIP protocol. Thanks to this, a user or resource can be localized by a Workflow at Grid layer or by another user or resource independently of the location or the current devices used, being able to choose the most suitable device if there are several, or to redirect a session from one device to another. A global identifier allows SIP to localize participants independently of their actual position or device used. In principle SIP is used exclusively to manage sessions, while the work performed in them is delegated to specific components that e.g. handle a voice or video conversation or a stream, IP is independent of the nature of the session being held. WP4.1 will provide means for other components to be able to trigger SIP sessions without restricting the type of session to be held. Thanks to this, any entity that has a SIP client at its disposal is able to be contacted and to contact other SIP clients, and redirect sessions to other devices (that also need to have SIP client capabilities). In addition it is possible for a peer to contact another peer using SIP. The ability for an external controller to put together two peers will also be possible, being able to manage the communication from outside of the peers, and being able to analyze its outcome. To this end, an interface will be developed in order to offer this capability to other modules that want to make use of it without having to implement specific functionality.

### 3.2.3. Technical mobility related experiences with MIPv6:

According to some experimental results obtained in a Test-bed developed to ensure the compatibility of MIPv6, IPv6 and IPv4 in relation with Web Services, some restrictions in terms of the operating systems that could be used at the time of writing this document were discovered. While the Linux OS has been shown to work without problems with Java/Axis and tomcat over a combined MIPv6/IPv4 environment, some issues arose with Windows series.

Windows Server 2003 doesn't support MIPv6 and therefore, although it may be thought to be a server and therefore not movable, a communication between this type of OS and a MN with MIPv6 will have a bigger overhead since no MIPv6 route optimization can be done.

Regarding the Windows XP and Pocket PC 2003 the MIPv6 implementation seems to work fine, however, name resolution with DNS can just be done over IPv4, which restricts the mobility capability of the nodes. In addition, the fact that the Pocket PC 2003 doesn't support java versions nor a .NET platform, that support IPv6, limits the use of Web Services with these technologies. As a result of this, and at least for now, Akogrimo will focus on using Linux based mobile nodes.

## 3.3. QoS

### 3.3.1. Taxonomy

Quality of Service can be defined in a very basic sense as consistent and predictable delivery of data. Different types of service have different requirements from the network. One application may require large bandwidth, while another, like a video conference, may require low delays.

Quality of Service in the Akogrimo network will allow a differentiation of various types of flows, allowing applications to select an appropriate set of QoS parameters including bandwidth, delay, jitter and packet loss. A short explanation of these terms follows:

- **Bandwidth:** rate at which bits are transmitted in the network[1].
- **Delay:** the amount of time between the start of sending and the arrival of a packet.
- **Jitter:** variation in the delay of packets.
- **Packet Loss:** discarding of packets at some network element due to operating conditions of the network.

### 3.3.2. QoS Bundles

Drawing from the requirements of the scenarios identified in WP 2.3 – Testbed Definition, as well as previous experience in QoS related projects, it was decided that 4.1 is to provide what we designate "QoS Bundles", instead of allowing individual parameter fine-tuning. Thus, QoS bundles appropriate for voice, video and data applications are provided.

The QoS bundles are constituted by well-defined services:

- **Signalling:** Signalling is traffic needed to maintain and support the network infrastructure, therefore it is the highest priority. It is time-critical and, in fact, essential to network operations as a whole. Typically its bandwidth requirements are very low.
- **Interactive real-time:** This is time-critical traffic that will be used mainly for video conferencing or audio communications. Interactive multimedia applications are very sensitive in regards to delays. The delays required for optimal functioning of interactive applications are less than 100ms. Latency and jitter also affect adversely voice communications. Another issue is packet sequencing. When two users are making a voice call, if some packets get delayed, they can arrive out of order, effectively arriving after the packets that are being output as sound by the application at that instant. Depending on the delay, the application, even though has the right packets, may have to discard them instead of reproduce them, for if it reproduced them, the results would most likely be unintelligible by the user.
- **Priority:** This type of traffic is not time-critical, but it is loss-sensitive, such as multimedia streaming, or some grid application data exchange. It is higher priority than Data Transfer, but has lower bandwidth available typically.
- **Data Transfer:** Data transfer is somewhere in between Priority and Best Effort. This type of traffic is not time-critical but may be loss-sensitive. While it is lower priority than Priority, it provides a larger bandwidth that is not available with Priority. Furthermore, out of order packets are typically no concern with applications that use Data Transfer.

[1] For digital communications purposes, bandwidth is, in reality, the rate at which symbols are transmitted, however it's mostly used for channel capacity, i.e. the rate of transmission of bits.

- **Best Effort:** As the name implies this service offers best effort. If network conditions are good, this should be fine for most applications. If the network is heavily loaded, BE will be the most affected. This is basically what Internet provides.

Table 2 shows the proposed QoS bundles for Akogrimo.

| Bundle 1 – Mixed, data + audio | Bundle 2 – High data + video | Bundle 3 – Mostly voice |
|---|---|---|
| Interactive – 10<br>Data – 100<br>Priority – 1<br>Signalling – 1<br>BE – 250 | Interactive – 20<br>Data – 1000<br>Priority – 200<br>Signalling – 1 | Interactive – 10<br>Priority – 1<br>Signalling – 1<br>BE – 250 |
| All units are in kilobytes per second | | |

**Table 2 QoS Bundles**

Should these bundles prove insufficient or inadequate, they can be easily modified or new ones created. The modification or creation of bundles is done entirely at the network layer and is totally transparent for higher layers.

### 3.3.3. QoS Services

For Grid applications to be able to make use of the QoS abilities of the Akogrimo network, they need to communicate with the QoS Broker. Since grid applications are based on Web Services, the obvious way to provide that functionality is to expose the required functionality of the QoS Broker as Web Services. The QoS Broker will have a WS which will allow it to receive requests, and, after acting on those requests, send the requesting party its answer as to whether the request was allowed or not.

The Execution Management System (EMS) component from work package 4.3 needs monitoring information from the network so that an SLA Controller may check if contracts are being upheld. A user's QoS bundle may be disrespected depending on the network conditions. Normally, the network only accepts new flows if there is available bandwidth. But in certain cases it may happen that the network is not able to sustain the ongoing flows QoS. For example, if the network load is high and there is an emergency call, the network will have to provide the emergency call with enough resources for its successful completion, and in doing so, other user's bandwidth may be deteriorated.

In order to keep the EMS informed of the QoS status of the user, periodical messages could be sent to the EMS, but that would pose scalability problems if the number of users grows. The solution found was to have the EMS assume that the QoS levels are being respected, and send a message when something happens that forces the degradation of user's services. This way, EMS is informed at all times of the QoS level of the user, and there is no necessity to use a significant amount of bandwidth with messages that merely state that "everything is ok".

An application may request a certain QoS bundle at any time. This bundle will have a certain duration which is also specified by the application. A running application that for some reason decides it needs a different QoS level may request a new QoS bundle at any time during its execution.

# 4. Grid Services Provisioning Constraints

Traditionally, Grid research was being focused on computing and data trends. Network layer was almost not taken into account on the Grid evolution. Akogrimo aims at filling the gap between the Grid and the mobile network layer. This linkage will optimize the Grid usage by improving it with new capabilities, new functionalities and features.

In Akogrimo, the network participates in the Grid infrastructure, by dynamically providing the capabilities the Grid requires. The network can be considered in that sense as a resource, like the software and storage are resources in the Grid environment.

In a mobile network, in which different types of connections, sudden disconnections, irregular connectivity and changes of location are possible, is obvious that the Grid infrastructure must be aware of the current networking capabilities. Furthermore, Grid services demand virtualization of network resources and may be able to manage, monitor and configure dynamically the network. Akogrimo architecture provides this by means of interactions between the components of WP 4.1 and WP4.3/4.4

- **QoS:** Due to the introduction of mobility, the bandwidth and guarantee of transmission between two peers is in general unknown and might be unstable. This is a totally new issue that the Grid needs to assimilate but also a territory that needs to be exploited to create new and better Grid services. In order to be able to carry out some of the tasks that take place at the Grid layer, the existence of a QoS mechanism and a link between SLA and QoS requests becomes necessary. As an example of how Grid induced QoS mechanisms could be useful the Akogrimo e-Health scenario can be helpful. In the Akogrimo e-Health scenario, when the doctor is videoconferencing with the patient and at the same time the doctor wants to download the patient records at his mobile device, the network provides an intelligent solution. The QoS accommodates the two flows (patient records and video conference) reducing the bandwidth for the video in the video conference but leaving the audio bandwidth unaffected, as the video is not essential for the purpose of the conversation. The intelligent network solution, which is provided to the e-Health grid service, is based on the communication held between the Execution Management Service at the grid layer and the QoS Broker at the network layer.
- **Security:** From the Grid point of view, operational VOs are created on the fly to carry out a certain task and after this is done the opVO splits up again. Therefore, powerful authentication and authorization are mandatory to ensure that the overall system is secure and business actives can be carried out without worries. Taking into account that users and possibly services roam across different administrative domains and networks, with different levels of security measures, it is important to authenticate the user from the very first moment in which he connects to a network and provide with necessary measures to protect the important data that is being transmitted (IPsec tunnels, IPsec P2P security…). Such a structure without any kind of network security would be totally unimaginable. An A4C system at the network layer is the most apt mechanism to take over the task of authenticating the user and providing him with means to get authorized to use other services in the network. In order to make a cross layered authentication and authorisation system possible, which starts when the participant attaches to the new network, there is a need for the A4C services and Grid VO management system to share a common infrastructure such as identity management.
- **Mobility:** Since nowadays Grid technologies have focused little in mobility and how to handle having different participants of the Grid moving around different networks. In

principle it is interesting that this movement is as transparent as possible to the Grid layer to avoid having to develop a lot of new methods or not standard technologies, however the fact that the Grid has a certain knowledge of the changing conditions to which the roaming participant is exposed is extremely fundamental for the creation of new highly innovative applications based on this technology. Therefore, context information such as bandwidth, type of connection, current availability or services available in the immediate location is extremely desirable.

# 5. Service Provisioning Protocols and Languages

## 5.1. Overview

From the Grid point of view and in the Akogrimo vision, the network is a mix of elements and heterogeneous infrastructures that should provide a clean and homogeneous interface to the upper layers, i.e. the Grid layers. If the network design succeeds in this objective, the network layer users will perceive the network as a homogeneous, compact layer that provides the services they need. Upper layers will, in turn, make use of these services to provide their intended functionality to the final users of the system.

From a high level and general perspective, basic services every network should provide include the following:

- Transport services
- Security services
- Access Control Services
- Quality services
- Signalling services

These services are explained in the following subsections.

## 5.2. Transport Services

The main goal of a network is to provide means to transport data from one device to another. The reference in network technologies is, of course, the Internet. The Internet was initially based on IPv4. However, the fast growth of the Internet has lead to the need to redesign this protocol in order to improve it and to allow it to give answers to the new requirements. That way, IPv6 [IPv6] was born, with a wider address space and many other improvements. The use of the IP family allows the interoperability of different, heterogeneous network technologies and devices, a key factor that is of special relevance in Akogrimo.

Both IPv4 and IPv6 are designed to static, fixed networks, where the point of attachment of a node to the network does not change. Addresses are associated with physical location through the network topology and changing the point of attachment requires reconfiguration in network equipment.

As ubiquity becomes more and more important and wireless network technology evolves, the need to overcome these limitations of IP grows. That is the reason why Mobile IPv6 was developed. MIPv6 extends IPv6 and allows devices to change their point of attachment. That way, a TCP connection established from a mobile node can survive the changes of location, even when the source and destination networks use different network technologies. Moreover, MIPv6 shows itself as a standard IPv6 layer to upper layers, so the mobility is done transparently to existing applications.

To allow mobility, some key concepts are defined within MIPv6 design. A mobile node (MN) has a home address (HoA) which is located in its home network. Any other node willing to send or receive data to or from the MN (known as correspondent node, CN) will use this address,

independently of the MN's location. The MN needs another address in order to receive traffic, valid within the network it is attached to. This address is called care-of address (CoA), and it is the effective address of the MN at any moment. The association between a MN's home address and its care-of address is called a binding. Every MN has a home agent (HA) which is aware of the corresponding MN's bindings.

With this setup, when a CN sends some packets to the MN, the HoA will be used. This will cause the packets to reach the HA if the MN is not located in its home network. If this is the case, the HA will check the MN's current binding and will forward every packet to the MN's CoA. The CN can be a regular IPv6 node, but if it uses MIPv6 it can be notified of the MN's binding allowing packets to be sent directly to the MN's CoA. This route optimization has a great impact on performance and is always desirable.

## 5.3. Security Services

Security has always been a major concern in network design. Security, as a service offered by the network to its users, is the ability of the network to keep the transported data secure. That means not only to keep the data private, so that only the intended recipient can read it, but also that the data is not manipulated and the sender is who he or she claims to be. This explanation translates into some of the key concepts used when talking about network security, that is:

- **Authentication:** The recipients can trust in sender's identity.
- **Confidentiality:** Transferred data will be correctly understood only by intended recipients.
- **Integrity:** Changes in the original data will be noticed at reception.
- **Non-repudiation:** Neither the sender nor the recipient can deny having sent or received a message they have actually sent or received.

There are several standards that address security at different scopes. To allow the aforementioned homogeneous vision of the network, several different security mechanisms and technologies will be used together to offer security as a complete service.

The different security mechanisms are associated with the layer they are aimed to secure. This will usually limit their scope:

- **Link layer security:** Several access technologies will be used, many of them being mobile. Each technology provides its own security mechanisms. Special care is needed for wireless access. In GSM/GPRS/UMTS a shared secret method is used to authenticate the user, and encryption algorithms ensure confidentiality of the traffic through the radio interface. UMTS extends GSM/GPRS security allowing the user to authenticate the network. WLAN, the other common wireless access technology, counts with its own security mechanisms, like WEP, WPA and WPA2, which provide encryption, authentication and integrity.
- **Network layer security:** The *de facto* standard in security at network level is IPSec, which stands for IP Security. IPSec can secure upper layers data or entire IP packets by means of IP tunnels. It is usually used to provide end-to-end security but it can also be used to enable network access security in a Virtual Private Network fashion.
- **Transport layer security: SSL/TLS** (Secure Socket Layer/Transport Layer Security) is the standard security mechanism for this. It can be seen as an additional layer placed between the transport and application layers, thus allowing the protection of application data in an end-to-end fashion. It uses public key certificates for endpoint authentication. The major drawback of SSL/TLS is its unsuitability to be used with UDP.

- **Application layer security:** There are several mechanisms to protect data in an application-oriented manner. First proposals were based on PGP (Pretty Good Privacy), which is based on cryptography algorithms. PGP was originally intended to e-mail use, but it is flexible enough to be used along with any type of data. Another widespread method for e-mail to secure data is S/MIME, an extension to the MIME (Multipurpose Internet Mail Extensions) standard. S/MIME makes use of X.509 certificates to secure application data. Many other application layer security mechanisms were developed (e.g. SNMPv3 for network management, etc.). Now, the current trend to use Web Services as an application infrastructure has forced to include also security in the Web Services infrastructure. In this context, there are a lot of security specifications in the Web Services Security area: WS-Security, WS-Policy, SAML, XML Signature and XML Encryption are examples of these specifications.

## 5.4. Authentication and Authorization Services

Although authentication and authorization are tightly related to security, they are described into their own sub-section, as they are also very important for mobility.

Authentication can be defined as the capability of the network to know who the user is and check his or her identity. Once the user is authenticated, authorization is needed to know what that user is able to do in the network.

As the user's identity is needed for almost every service offered by a network, authentication is performed as soon as possible, usually when the user first accesses the network. As opposed to link layer security mechanisms, whose main objective is to secure the physical access of the user to the network, authentication mechanisms try to secure the access of the user to the network in a higher level manner. At this higher level, the network does not distinguish the different technologies used for physical access, so a common, homogeneous mechanism to authenticate the user is needed.

In these scenarios, the Protocol for carrying Authentication for Network Access is especially suitable, since it uses IP-based protocols. PANA [PANA] was designed by the IETF to provide this access network-independent mechanism. PANA relays on another protocol, EAP (Extensible Authentication Protocol), which is also designed by the IETF. EAP is very powerful thanks to its flexibility, which makes it suitable to be used for several different authentication methods. EAP packets are carried as payload in PANA's ones.

As stated before, authentication and authorization are also very important for mobility. More precisely, they enable interdomain mobility, i.e. the capability of the user to roam through different administrative domains. When a user visits a foreign network, the provider of the visited network needs to know about the user to allow him or her to access the network and use its services. However, there is no data about the user in the visited network, and the authentication must be accomplished contacting the user's home network. A4C (Authentication, Authorization, Accounting, Auditing and Charging) architecture, based on the Diameter protocol [DIAM], is used to do this, and in general, for carrying out a Single Sign On objective and centralized point for authorization, accounting, etc.

## 5.5. Quality of Service

Every application in a network is affected by the quality of how the needed data are transported. Aspects like delay, jitter, bandwidth, etc. limit the application communication capabilities, having an impact on application behaviour. Each application is affected by each aspect of the communication in a different level. Quality of Service (QoS) is the ability of the network to identify different kinds of traffic and their requirements, and to setup itself in order to fulfil them.

There are several ways to do so, including the prioritization of some traffic flows over others or the reservation of the resources needed to guarantee communication conditions before the communication itself takes place.

Several models and mechanisms have been designed to add QoS to different network technologies. As the use of IP increases, a lot of effort has been put to enable QoS on IP networks. Two models, both designed by the IETF, are more commonly used: the Integrated Services (IntServ) model and the Differentiated Services model (DiffServ).

IntServ provides a signalled-QoS model. This model is called signalled because the endpoints of the communication must signal the network before the communication between them starts. With this signalling, an application willing to establish a session with another one, first informs the network about its communications requirements and the characteristics of its traffic in order for the network to perform a resource reservation. This reservation ensures that the application requirements are met in an end-to-end fashion. This implies resources to be reserved in every router in the data path.

To perform this previous resource reservation, the Reservation Protocol (RSVP) is used. A router in the data path will be informed about QoS requirements using this protocol. The router then checks the resources available and decides to or not to accept the request. Because of routers storing all the needed state for each established session, the IntServ model has limited scalability.

To overcome IntServ model's limitations, DiffServ was designed. It follows a provisioned-QoS model, where service classes are defined, along with their respective QoS requirements. Using a DiffServ model, the edge routers of a network will mark the traffic packets as belonging to the service class that better fulfils that traffic's particular requirements.

Network elements in the core network are configured to deal with the different service classes in a pre-defined way. A core router will always do the same with every packet of a given class. That way, routers do not need to maintain any state about established sessions, but only their expected behaviour when packets of the different classes arrive. Once a packet is routed, delayed or discarded, it is forgotten and the next packet is processed.

The Akogrimo network will use a hybrid IntServ/DiffServ network. Access Networks will work based on the IntServ model, which allows end-to-end QoS reservations. For overcoming the IntServ limitations, the Core Network will use DiffServ. This allows the Core Network to aggregate all the flows of the same type and transport them to the destination Access Network, where the IntServ model is used once again. This hybrid mechanism is further explained in D4.1.1 – Consolidated Network Layer Architecture in sections 2.3.1 and 2.4.1.

## 5.6. Signalling Services

The network should also provide to upper layers a signalling infrastructure capable to fulfil signalling requirements for applications. Signalling is commonly associated with the concept of *session*, a relationship, with a limited duration in time, between two or more endpoints that allows the communication between them. Signalling concepts on modern networks are inherited from classic signalling scenarios, like telephony networks.

The first widely used signalling protocol was H.323 [H323], a recommendation from the ITU-T designed to enable multimedia communications over packet-based networks. It is commonly used in Voice over IP. H.323 has gone through several versions, and it now covers many aspects of multimedia communications, as network interoperability, security, codec negotiation, and additional services like call transfer and call forwarding. All this features make H.323 very complex and difficult to work with.

IETF has also put a lot of effort on signalling, and the result is the Session Initiation Protocol (SIP). SIP is becoming very popular and its use is growing because it is far less complicated than

H.323. SIP is designed to establish, modify and tear down sessions in IP networks. It has a HTTP-like syntax and provides some built-in services as user location. It does not specify the kind of session or the transport protocol that will be used. This feature gives SIP a great flexibility, which makes it suitable to be used along with any session-based application.

As with H.323, SIP is commonly used for audio/video communications. To do this, SIP is combined with other protocols, like the Session Description Protocol (SDP) and the Real-time Transport Protocol (RTP). SDP is used to define session-specific parameters related to the communications, as addresses and ports and the audio/video codecs to be used. SDP descriptions are included in SIP messages at session-establishment time to negotiate and setup the incoming communication details.

After the session has been established and the communication has been setup, RTP is used to effectively transport the media data packets between the communication endpoints. In addition, the Real-time Transport Control Protocol (RTCP) can be used to monitor the status of the communication being held.

# 6. Akogrimo Service Provisioning Architecture

## 6.1. Overview

The Akogrimo project aims to integrate two hitherto disparate fields: grids and networks. Grids have stopped being highly specialized applications, used only in a few high performance computing centres, and are becoming more widespread. Many people still associate grids with high performance computing, but in reality they are more about the sharing of resources, be they CPU cycles or disk storage, for example.

Networks have also changed drastically in recent times. Only ten years ago very few individuals had Internet connection available at home. Nowadays you can read your email while waiting for the next plane at the airport using wireless LAN.

## 6.2. Network Service Provisioning

The whole Akogrimo project will use services provided by the network layer. Some of those services will be transparent to the grid layer, such as the transport and security services. Others will involve some degree of cross layer interaction between QoS and SIP on the network side, and Grid infrastructure or applications on the other side.

The network services that will be of interest for the grid layers are the quality of service and SIP services. Grid services or applications may require Quality of Service for their optimal functioning, thus it is required that the grid layer may control in some way the QoS that it uses. Work package 4.4 or Akogrimo applications will also require some control over SIP sessions, like the ability to start a new session.

The QoS and SIP services that have been identified as priorities for the first phase of the project are:

i. Starting a SIP session
ii. Requesting a QoS bundle
iii. Getting the status of a user's QoS (for SLA purposes)
iv. User Location (discussed in section 7)

In order for grids to be able to use the network as a resource the network layer will have to provide a selected number of services to the grid layer.

The ideal solution would be to allow the sharing of network resources and functionalities as if they were part of the grid. An OGSA compliant toolkit such as Globus Toolkit 4 may enable us to share network resources and functionality in a grid-like manner and that would allow a superior integration of network and grid services. Work package 4.1 plans to research the feasibility of that solution.

For the first phase of the project, the approach that has been followed is to develop Web Service interfaces for the functionalities that are considered to be the most important. Taking, for example, the eHealth scenario, the network should provide the ability for grid applications to use SIP capabilities for a voice call requested by a patient in need of medical attention, as well as assure that that call is not disturbed nor its quality degraded by an overloaded network.

## 6.3. Web Services

Work package 4.1 makes interacting with SIP and QoS easier for grid layers by providing them with Web Services that uses the SOAP protocol for exchanging messages, allowing grid layers to use more familiar tools and protocols to control key network components. Albeit the Web Services are limited in their functionality when compared with using the native network protocols, they do provide the necessary means for grid layers to make SIP or QoS requests.

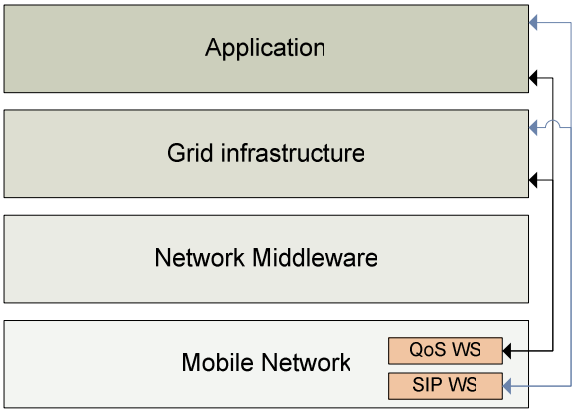


**Figure 2 Cross layer QoS and SIP**

Following this approach, a cross-layer interface between the network layer and grid layer is created. This adds some complexity to Akogrimo, but the benefits of a tighter integration outweigh the minor drawbacks.

The QoS and SIP WS may be located either in respective network elements, or may be implemented in another machine running as a dedicated WS server, communicating with the network elements it controls over the network. A dedicated machine running WS presents scalability problems, since it will receive requests which have as destination multiple network elements, while the first solution increases the processing load of the respective network elements. The best approach will be decided when there is enough performance data for making an informed decision.

# 7. User Location

## 7.1. Overview

User Location (UL) is the capability of detecting the position of a user. Several Akogrimo scenarios depend on UL for the scenario workflow to work properly. Furthermore, the Akogrimo scenarios precision requirements of the UL service are quite high – no more than 2 meters error.

Work package 4.2 will be using RFID for providing user location. However RFID is able to detect that a user entered or left a room, but is not able to provide its exact location. Another possibility is GPS, but that implies that the user carries a GPS device.

This User Location service can be used as a last resort, when RFID or GPS are not options, due to either requirements of scenarios or limitations of those technologies.

## 7.2. Available technologies

There exist several technologies which allow user location. However, these technologies are usually not as precise as necessary, and in some cases its implementation is difficult and/or impractical.

- **Wireless LAN:** hotspot triangulation could be performed, however it is not very precise and not much work has been done in this field. Also, it only works if the user is covered by more than one hotspot (preferably three or more), which may not happen all the time.
- **LAN:** knowing the map of LAN sockets of a particular room or location, the user's physical location is determined with minimal error, however it only works for wired connections.
- **GPS:** GPS does not provide the needed error margin, and it would implies the user having to carry a GPS device at all times.
- **RFID:** RFID enables a system to know when a user passes through an RFID detector. If the detector is placed in the entrance of a room then it is possible to say that the user has entered or left the room.

## 7.3. Implementation of the UL Service

Since it was impossible to find a UL technology available nowadays that meets the requirements of the project, an alternate solution had to be found.

That solution is a "dummy" user location service that will provide precise user location using fictional data. Using this solution, the applications that require so will have precise user location, scenario workflows may function properly, and in the future, it will be possible to substitute the "dummy" user location service with a real solution.

### 7.3.1. UTM Coordinates

The UTM (Universal Transverse Mercator) coordinate system [UTM] was the chosen coordinate for the UL Service. Its choice was based on some of its advantages over angular systems:

- constant distance relationship anywhere on a map
- metric based
- no conversions between minutes or seconds

- easy to read format

An example of an UTM coordinate is 14T 654321 123456, where 14T is the zone, 654321 is the easting and 123456 is the northing.

The UTM coordinate system divides the globe in 60 zones, which start at the International Date Line, and are numbered from 1 to 60. Each zone is further divided in horizontal bands which are represented by a letter from C to X. Letters I and O are not used to avoid confusion with numbers one and zero.

Each zone has a central meridian with an arbitrary value of 500,000. This value ensures that negative values will never exist, since each zone is at maximum 674,000 metres wide.

Eastings are referenced to the central meridian of the zone. Northings are measured relative to the equator, when in the northern hemisphere, or measured relative to the South Pole when in the southern hemisphere. Both eastings and northings values are measured in metres.

Figure 3 shows the map with UTM zones which is presented by the GeoMag software [GEO], with which a user can find out the UTM coordinates of a location.

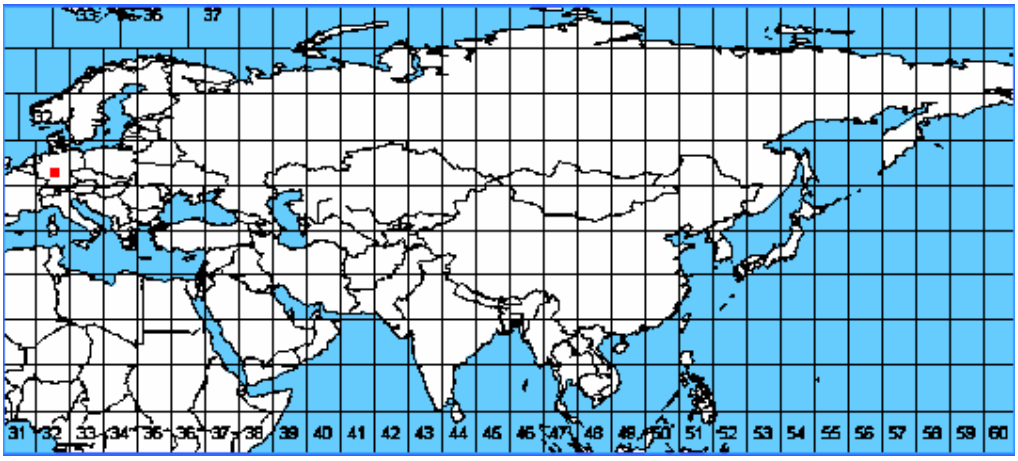


**Figure 3 UTM map**

## 7.3.2. UL Web Service

The Akogrimo User Location Service is a Web Service that requires a user identifier as an argument. It will then lookup the user's location in its internal fictional database, and finally it will return the user location to the application that invoked it.

The UL Web Service is a compromise solution to a complex problem. The user location precision required by Akogrimo scenarios is too high for present technologies to provide, and building a new user location mechanism is out of the scope of the Akogrimo project.

By using fictional data fed to a web service which then returns UTM coordinates with precision of one metre we fulfil the precision requirements of Akogrimo. Furthermore, if a new technology emerges that is suitable for Akogrimo, the web service can be modified to use the real UL data instead of the fictional database, without impacting programs built upon the UL web service.

# 8. References


[AAA] C. de Laat, G. Gross, L. Gommans, J. Vollbrecht, D. Spence, "Generic AAA architecture" RFC2903 URL:http://www.ietf.org/rfc/rfc2903.txt Last visited 11/11/2005

[DIAM] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko. "Diameter Base Protocol", IETF RFC 3588, September 2003. URL: http://www.ietf.org/rfc/rfc3588.txt Last visited 11/11/2005

[GEO] GeoMag, Geographic Magnetic Calculator, URL: http://www.resurgentsoftware.com/geomag.html Last Visited 7/11/2005

[H323] H.323 – Packet based multimedia communication systems, URL: http://www.itu.int/rec/recommendation.asp?type=items&lang=E&parent=T-REC-H.323-200307-I Last Visited 11/11/2005

[IPSEC] S. Kent, R. Atkinson, "IPsec - Security Architecture for the Internet Protocol" RFC2401, URL: http://www.ietf.org/rfc/rfc2401.txt Last Visited 11/11/2005

[IPv6] S. Deering, R. Hinden, "Internet Protocol version 6", RFC2460, URL: http://www.ietf.org/rfc/rfc2460.txt Last Visited 11/11/2005

[MIPv6] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6" RFC3775, URL: http://www.ietf.org/rfc/rfc3775.txt Last Visited 11/11/2005

[PANA] Protocol for Carrying Authentication for Network Access, URL: http://www.ietf.org/internet-drafts/draft-ietf-pana-pana-10.txt Last Visited 11/11/2005

[RTP] H. Schulzrinne, S. Casner, R. Frederick,V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications" RFC 3550, URL: http://www.ietf.org/rfc/rfc3550.txt?number=3550 Last Visited 7/11/2005

[SDP] M. Handley, V. Jacobson, "SDP: Session Description Protocol" RFC 2327, URL: http://www.ietf.org/rfc/rfc2327.txt Last Visited 7/11/2005

[SIP] J. Rosenberg/H. Schulzrinne/G. Camarillo/A. Johnston/J. Peterson/R. Sparks/M. Handley/E. Schooler., RFC 3261 "SIP: Session Initiation Protocol", URL: http://www.ietf.org/rfc/rfc3261.txt?number=3261 Last Visited 11/11/2005

[UTM] UTM – Universal Transverse Mercator Geographic Coordinate System, URL: http://geology.isu.edu/geostac/Field_Exercise/topomaps/utm.htm Last Visited 7/11/2005