D4.1.1

Mobile Network Architecture, Design & Implementation

Version 1.0

WP 4.1 Consolidated Network Layer Architecture

Dissemination Level: Public

Lead Editor: Nuno Inácio, IT-Aveiro

7/11/2005

Status: Final

SIXTH FRAMEWORK PROGRAMME

PRIORITY IST-2002-2.3.1.18

Grid for complex problem solving

Proposal/Contract no.: 004293

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.

c. For the avoidance of doubt, where the work is a musical composition:

    i. **Performance Royalties Under Blanket Licenses**. Licensor waives 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.

    ii. **Mechanical Rights and Statutory Royalties**. Licensor waives the exclusive right to collect, whether individually or via a music rights society 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).

d. **Webcasting Rights and Statutory Royalties**. For the avoidance of doubt, where the Work is a sound recording, Licensor waives 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).

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.

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 credit as required by clause 4(b), as requested.

b. If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or Collective Works, You must keep intact all copyright notices for the Work and provide, reasonable to the medium or means You are utilizing: (i) the name of the Original Author (or pseudonym, if applicable) if supplied, and/or (ii) if the Original Author and/or Licensor designate another party or parties (e.g. a sponsor institute, publishing entity, journal) for attribution in Licensor's copyright notice, terms of service or by other reasonable means, the name of such party or parties; 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.

5. Representations, Warranties and Disclaimer

UNLESS OTHERWISE MUTUALLY AGREED TO BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE MATERIALS, 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, 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 Based on work from WP3.1, WP4.2, W4.3, WP4.4 Integration work on WP5.1 may depend on this deliverable

Contributors	**Reviewers**
Patrick Mandic (UStutt-RUS) Nuno Inacio (IT Aveiro) Rui L. Aguiar (IT Aveiro) Susana Sargento (IT Aveiro) Dirk Haage (UPM) Vicente Olmedo (UPM) Víctor A. Villagrá (UPM) Jose Ignacio Moreno Novella (UPM) Isabel Alonso (TID) Arantxa Toro (TID)	Internal review by WP4.1 participants. Review by partners external to 4.1: Per-Oddvar Osland (Telenor) Cristian Morariu (University of Zurich) Juan E. Burgos (TID) Stefan Wesner (UStutt-HLRS) Juergen Jaehnert (UStutt-RUS)

Approved by: QM

Version	Date	Authors	Sections Affected
0.1	8/3/05	Nuno Inácio	All (Table of Contents)
0.2	27/6/05	All	All
0.3	11/7/05	All	Updates to all sections
0.4	10/9/05	Dirk Haage, Patrick Mandic	PBNM, Security updates
0.5	20/10/05	Nuno Inácio	Updates to Network Architecture, Quality of Service; ready for internal review

0.6	3/11/05	All	All sections updated after review by Akogrimo partners
1.0	7/11/05	Nuno Inácio	Final version

Executive Summary

This document defines the Akogrimo network architecture and depicts the corresponding design and implementation of each component in which this architecture is divided. WP4.1's main task is to create the substrate that transports the logic generated by the above layers. Differentiating characteristics of Next Generation Networks (NGN) are addressed in this architecture with the added incentive of embracing and accommodating Grid technologies on top of it.

To start off, basic requirements of the architecture such as mobility, network security, QoS, Network Management, Network Service Layer Provisioning are reasoned in the document.

In order to carry out such a challenging task, the architecture has been created dissecting it in three different zones with different goals and characteristics. These zones are: the Core Network, the Access Network and the Mobile Terminal. Each component of the architecture is grouped in one of these zones according to the job it develops. In addition, these components reflect the requirements imposed previously in the document and follow the trend generated by the D3.1.1 in which coarse behaviour guidelines where provided for the correct interoperation between all the WP4.x packages. For each one of them a description is provided.

The core of the document tackles the description of the design, functionality and implementation of the building pillars that this network infrastructure comprehends. For the sake of clearness this is divided in different sections: Mobile Access Infrastructure, Network Security, QoS, PBNM, Network Service Provisioning, SIP Mobility.

Table of Contents

List of Figures

List of Tables

Abbreviations

3PCC	3rd Party Call Control
3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
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
AR	Access Router
ASN.1	Abstract Syntax Notation number One
BA	Binding Acknowledgement
BU	Binding Update
CIM	Common Information Model
CN	Core Network
CoA	Care-of Address
COPS	Common Open Policy Service Protocol
CPU	Central Processing Unit
DB	Database
DiffServ	Differentiated Services
DoS	Denial of Service
DSCP	Differentiated Service Code Point
E2E	End-to-end
FQDN	Fully Qualified Domain Name
HA	Home Agent

HO	Handover
FHO	Fast Handover
HoA	Home Address
IETF	Internet Engineering Task Force
IKE	Internet Key Protocol
IMS	IP Multimedia System
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
MT	Mobile Terminal
MTIHO	Mobile Terminal Initiated Handover
NGG	Next Generation Grid
NGN	Next Generation Networks
NIHO	Network Initiated Handover
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
PM	Policy Manager
QoS	Quality of Service
QoSB	Quality of Service Broker
RSVP	Resource-Reservation Protocol

RTP	Real-Time Protocol
RTSP	Real Time Streaming Protocol
SA	Secure Association
SDP	Service Discovery Protocol
SIP	Session Initiation Protocol
SIP UA	SIP User Agent
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

Definitions

Accounting

Accounting performs two main tasks. The first is collecting data on resource consumption from the services via a metering component while the second task is retrieving stored accounting data whenever this is requested by a legitimate entity.

Auditing

Auditing defines the process of storage and retrieval, when needed, of information on events taking place in the system, history of the service usage, SLA (Service Level Agreement) compliance, and customer charging and tariff schemes applied.

Authentication

The authentication mechanism defines a process for verifying a user's identity.

Authorization

Authorization is the process of decision on an entity's allowance to perform a particular action or not. The Authorization decision depends on service specific attributes (e.g. service class for QoS service, device requirements) and user-specific attributes (e.g., name, affiliation to a certain group, age, etc.).

Charging

Charging is the task of calculating the price for a given service consumption based on accounting information. Charging maps technical values in monetary units and then applies a previously established contractual agreement between service provider and service consumer upon a tariff.

Contract

A legal agreement between a subscriber and a provider, stipulating the benefits that should be delivered to the subscriber.

Profile

A group of attributes associated with a user which provides information necessary to access services.

Provider

An entity that provides services to users under a contract. The provider may offer network and/or application services, as well as content.

QoS Broker

The network entity that handles quality of service.

Quality of Service (QoS)

A quantitative and qualitative measure that determines a subscriber's degree of satisfaction. The network must be able to provide different levels of service to different applications.

SAML artefact

A SAML artefact is a piece of data produced by a SAML Authority regarding either an act of authentication performed on a user, attribute information about the user, or authorization data applying to the user with respect to a specified resource.

1. Introduction

From the very beginning, the Akogrimo project has been type-casted as a Next Generation Grid (NGG) that is well aware of the underlying network utilized. This definition certainly provides a glimpse of an intended goal pursued however, biased towards the Grid field giving the impression of having a fully innovative NGG, which is able to communicate with a regular, ordinary and lackluster network infrastructure. Far from this, the network infrastructure strives not only to leverage a blueprint of a network-aware NGG but also grow strong in the field of Next Generation Networks (NGN) by extending the concept with the contribution of the Grid technology. Some Classical NGN characteristics can be found in Akogrimo such as:

- Types of media access technologies are not considered, instead an all-IP-access-network-independent concept of followed.
- Different kinds of traffic are accommodated in the network by means of QoS management.
- Different types of mobility are provided: An application transparent, access network independent terminal mobility is provided using MIPv6. User/session mobility gives an orthogonal dimension to the concept of mobility by detaching it from the terminal. These two types of mobility are independent from each other. A third type of mobility is provided by roaming agreements between different networks.
- Authentication, Authorization, Accounting, Auditing and Charging (A4C) are provided in order to enable the introduction of commercialization of services.
- Policy-based network management.
- Security is a must.

Similar paths are followed by NGNs such as the IP Multimedia Subsystem (IMS) created by the 3GPP (or the parallel one created by it homologue, 3GPP2). IMS was created in order to promote the migration from a circuit-switched technology that had become a commodity for voice communication operators towards a new packet-switched platform that could make it worth for them to make the investment profitable. IMS is based in IETF specifications, in a few words we could say that the mobile wireless telephony comes together with the IETF packet-switched internet. In this context, IMS is strongly oriented to multimedia services. On the other hand, Akogrimo's network tendency is not so much focussed on multimedia services (since they are already being investigated by other entities) as it is on Grid provisioning. Classical NGN characteristics are here also oriented towards the interaction with Grid components (e.g. Virtual Organizations). A4C, QoS, Security, Roaming, Identity management and so on, are developed in conjunction with the Grid layer to enable a nursery for new applications and promote the commercial use of new Grid technologies over new Network infrastructures

2. Mobile Network Architecture, Design & Implementation

2.1. Overview

The Akogrimo Description of Work defines a number of requirements and challenges for the Akogrimo project. These requirements were further refined in ID2.3.1 – Initial Testbed Description and in D2.3.1 – Testbed Description. This deliverable takes into account those requirements and correlates them with D2.2.1 – Report on the State of the Art. By analysing the requirements in light of what are the best technologies and solutions today, it was possible to achieve a network layer design that fulfils most of the requirements and, in doing so, allows the Akogrimo project to advance towards its goal. This chapter presents the requirements from a network point of view, as well as an overview of the projected Akogrimo network.

The Mobile Network Architecture layer represents the foundations upon which other Akogrimo layers are built. It will use existing mobility management solutions already proven in other projects, such as Moby Dick [MD] and Daidalos [DAI] updated to today's needs and adapted to NGG necessities. The envisaged network will support seamless mobility in a heterogeneous network environment, along with security and quality of service. It will also allow the provisioning of Grid based services integrated with the underlying network.

The IPv6 protocol [IPv6] will be the basic building block, what we might call an abstraction layer, which allows a single network architecture to support multiple access technologies. Furthermore, the use of Mobile IPv6 [MIPv6] will allow the required terminal mobility. Akogrimo will focus on Ethernet and Wireless LAN technologies, since the infrastructure required for other technologies (e.g. UMTS) is very expensive. However the use of IPv6 guarantees that, should the need arise, those other technologies can in the future be integrated without any problems in the Akogrimo network.

2.2. Requirements

2.2.1. Mobility

Akogrimo aims to develop a mobile Grid environment, so one obvious requirement is mobility. However, there are different types of mobility that play different roles, and the Akogrimo network must support the various types of mobility. A brief explanation of each of the mobility types considered in Akogrimo follows.

2.2.1.1. Terminal Mobility

Terminal mobility enables a terminal to remain connected to the network even if it changes access point or access technologies.

SIP alone is not enough to guarantee seamless terminal mobility, for if a non-Mobile IPv6 capable terminal changes access point, it loses connection to its previous network and gains a new IP address in the new network. In practice, that means that all its ongoing communications before the change, are stopped and have to be restarted.

Terminal Mobility is discussed further in section 3.

2.2.1.2. User Mobility

User Mobility enables the user to access network services or resources independently of the user's terminal. A user-oriented security and authentication framework is responsible for this.

2.2.1.3. Session Mobility

Session mobility enables a session to continue without interruptions regardless of changes in points of attachment to the network, user terminal changes or even if the session is transferred from a user to another (e.g. if you want to redirect your display from your laptop to a huge screen). Session mobility can be achieved through the use of the SIP protocol. Session Mobility is further discussed in section 7.3.

2.2.2. Network Security

In conventional access and transport network environments the notion of network security usually refers to functionalities and tasks bottom up from the physical up to the "AAA layer" – e.g. in the IETF spirit. On the other hand, in conventional Grids there is a security framework centred on WS security and corresponding technologies. However, up to now, there are basically no considerations to possibly make both security fields "aware of each other". For example, there are hardly any Grid projects making use of an IETF oriented AAA infrastructure. On the other hand, there are equally only now network projects using WS oriented security technologies such as SAML. Within this context, Akogrimo strives to develop an architecture which makes Grids network aware, even mobility aware – and vice versa.

2.2.3. Quality of Service

Quality of Service is assuring that a client will get the service he paid for without restrictions, be it simple web browsing, communicating with a grid service or performing video conferences. In the Akogrimo eHealth scenario, in particular, quality of service is of capital importance, since any failure in meeting applications requirements can cause problems to the patient.

2.2.4. Network Management

The Akogrimo network will have a large number of machines in order to support itself. Traditionally, managing such a network can be a complicated issue to the administrator, so in Akogrimo a Policy Based Network Management system will be used to relieve the burden of the administrator. The PBNM will send policies to specific network elements, which will then act according to those policies.

2.2.5. Network Service Layer Provisioning

The Akogrimo project aims for the integration of a next generation grid with a heterogeneous network environment with quality of service. To that end, the network layer will have enhancement points which will allow the exposure of network layer functionalities to the grid infrastructure.

Of particular importance is the need to provide QoS and SIP functionalities to Grid layers. To that end, Web Services will be provided using the SOAP protocol for allowing QoS reservation and SIP call requests from the Grid layers. More information about these Web Services can be found in D4.1.2.

2.3. Network Architecture

2.3.1. Basic Concepts

The Akogrimo network architecture follows a layered approach and is comprised of a Core Network (CN), several Access Networks (AN) and a number of Mobile Terminals (MT). The terminals connect to the access networks and these in turn, communicate with the main core network.

The Akogrimo network will support terminal mobility, which means that besides normal wired connections it will also support wireless communications. The use of IPv6 allows the network management components to communicate with users' terminals using a standard protocol irrespective of the network access technology the terminal is using, be it Ethernet, 802.11 or other.

A simplified network-oriented view of the Akogrimo layers is present in Figure 1:

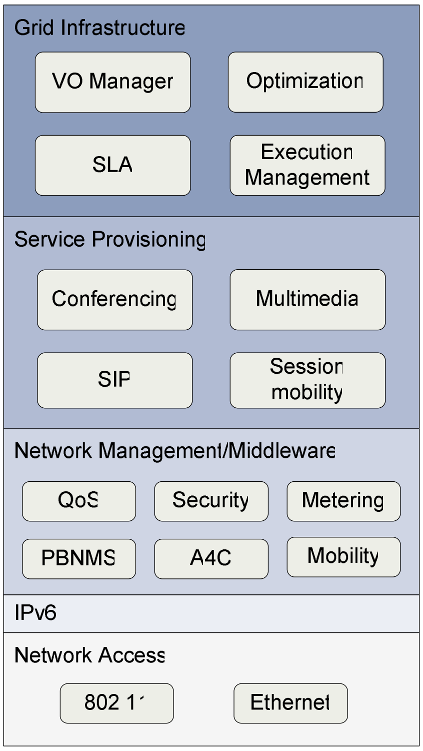

Figure 1 – Layered view of Akogrimo

Figure 2 – Akogrimo Network is a diagram of a possible physical deployment of the Akogrimo network:

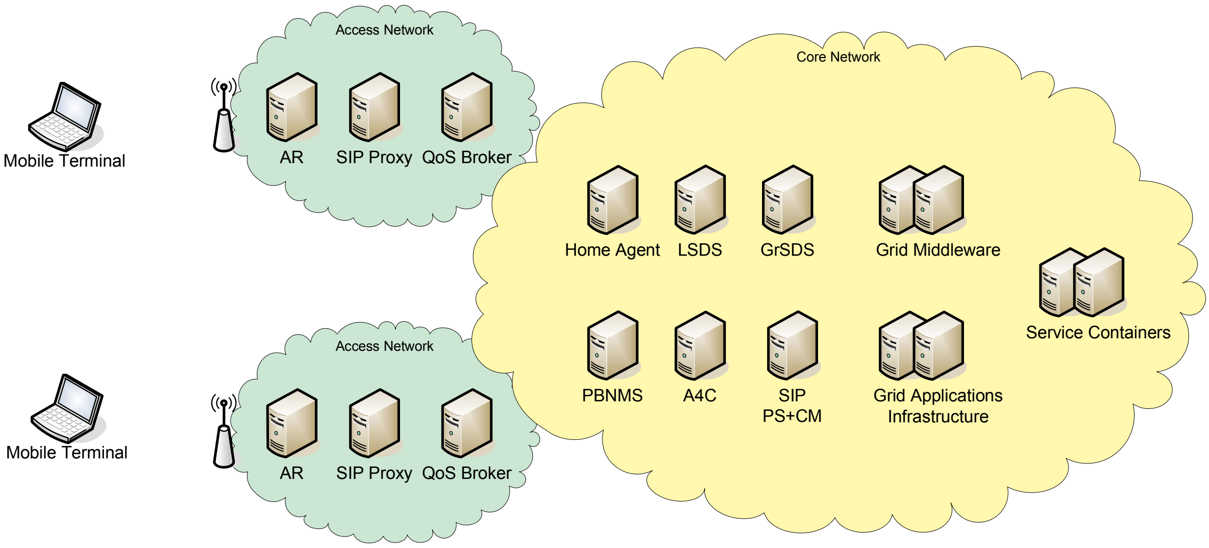

Figure 2 – Akogrimo Network

Figure 2 and relevant components present in it will be explained in upcoming sections of this document.

End-to-end QoS is a requirement, therefore Akogrimo will support IETF's IntServ model. However, because of IntServ scalability problems, the Akogrimo Core Network will work based on IETF's DiffServ model. The Akogrimo network is, thus, a hybrid network, with IntServ based access networks which will provide per-flow QoS granularity and a DiffServ core network which aggregates different flows with similar QoS requirements into a single class of service. This will enable the Akogrimo network to provide end-to-end QoS while remaining scalable.

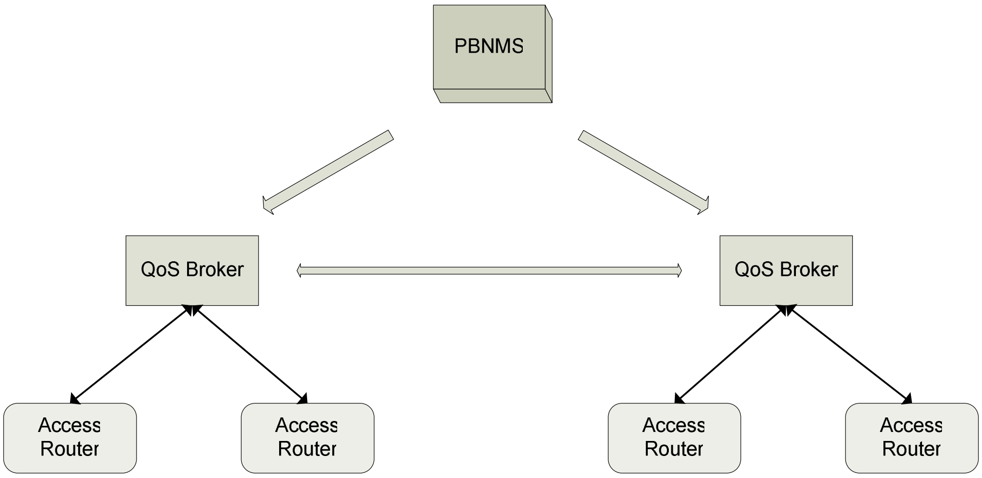

Figure 3 – QoS components relations

QoS will be implemented by not only the QoS Broker, but also the PBNMS and the access routers. Figure 3 shows the relations between these components. The PBNMS sends network policies to the QoS Brokers. The QoS Brokers manage all network flows in the Akogrimo network. They are all interconnected with each other. Each QoS Broker responds to requests from access routers it's responsible for and sends them the respective decisions. The access routers do the actual enforcing of the decisions that the QoS Brokers have previously made.

2.3.2. Core Network

The Core Network is the central point in the network. It connects all Access Networks and controls the user's identity, security, authentication, authorization, accounting, auditing, charging, multimedia services and mobility. It is also responsible for providing users with access to Grid services.

In Akogrimo we assume that the Core Network always has available resources for network communications, therefore we don't have a great control of traffic inside the CN. This is due to the fact that in today's networks, ISPs usually have a very low percentage of use of their CN, and that situation is not likely to change in the near future.

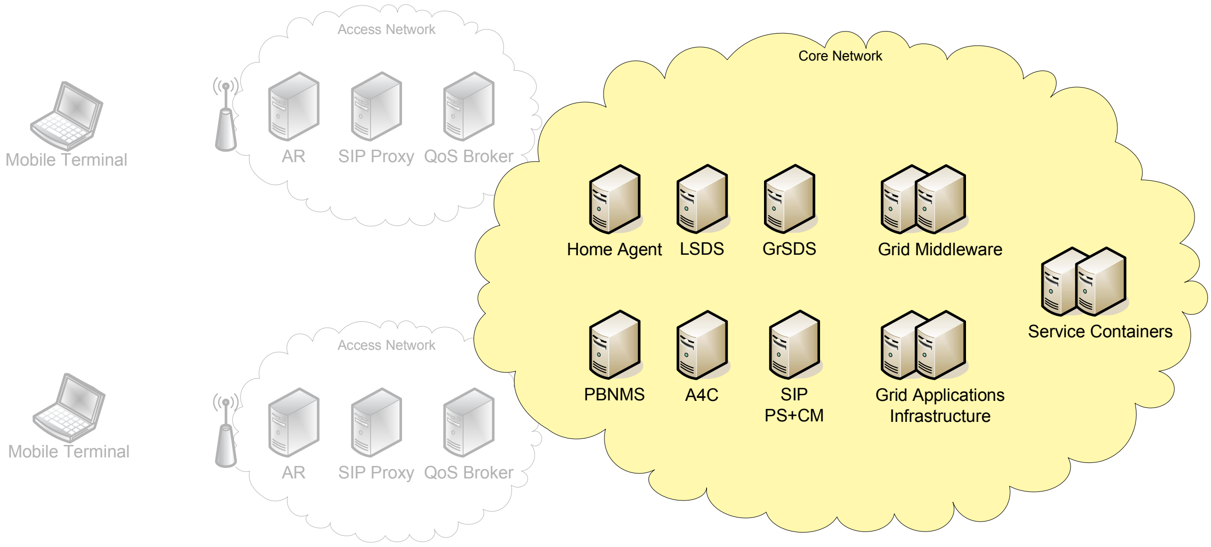

Figure 4 – The Core Network

The CN holds network components such as the A4C Server, the mobile IPv6 home agent, the PBNMS or the SIP Server. Grid infrastructure components will either reside in the CN or in a network with a high capacity connection to the CN and with agreements with the network service provider in order to have optimum network performance. For simplicity reasons we depict them in the CN independently of their actual physical location.

2.3.3. Access Network

The Access Network allows the connection of terminals using different access technologies (Ethernet, 802.11) and communication with the core network. The core network has several access networks. Several user terminals may connect to a given AN.

The AN is comprised of at least one Access Router and one QoS Broker. The SIP Proxy is part of the SIP Server which is located in the CN, although for scalability reasons the proxy module may be separated and distributed among the various access networks (which is how it is depicted in Figure 5).

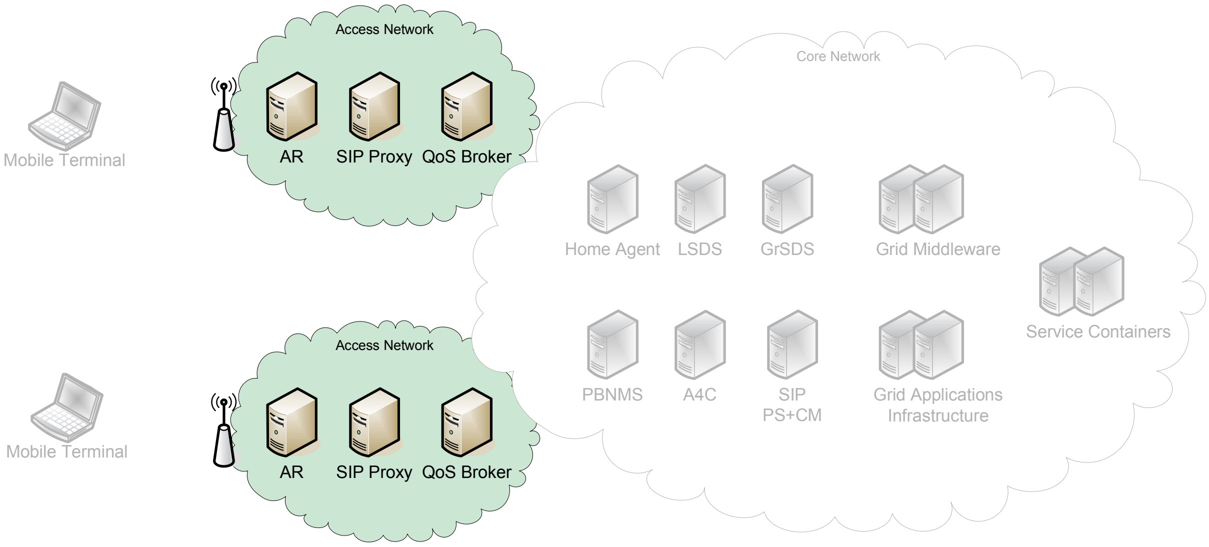

Figure 5 – Access Networks

2.3.4. Mobile Terminal

The mobile terminal is the device used to connect to the Akogrimo network; it may be a notebook, PDA or even a normal, non-mobile PC. Either way, for simplicity reasons, it will be referred to as the mobile terminal, since it is the user's computer and the software installed on it has support for mobility irrespectively of the kind of computer it is. The mobile terminal can connect to access networks and make use of services provided by both the access and core networks, as well as grid services.

2.4. Network components description

2.4.1. Access Router

The Access Router acts as an interface between wired/wireless terminals and the core network. A single AR may support different access technologies. The remainder of the network will be able to communicate with different mobile terminals in the same way, regardless of the technology they are using for network access.

The Access Router also provides network management components (such as QoS Broker, for example) with a uniform way of managing a heterogeneous network environment such as the one which will form the Akogrimo network. Figure 6 shows a functional view of the AR.

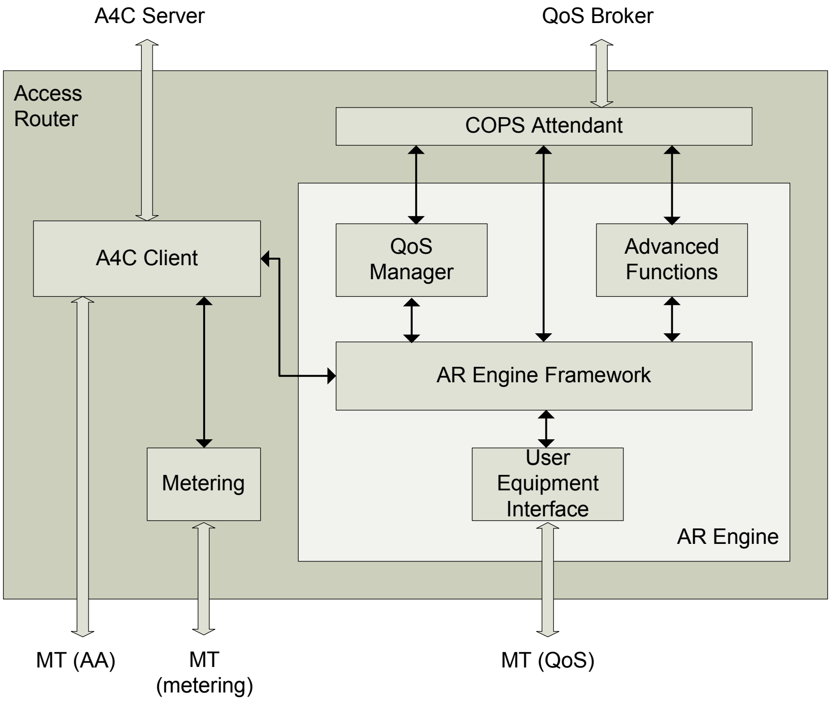

Figure 6 – Akogrimo Access Router

The Access Router is comprised of the AR engine which provides most of its functionalities. It also incorporates an A4C Client which communicates, using the Diameter protocol, with the A4C Server for authenticating users and for sending accounting information. The Metering module makes basic per-flow metering and communicates its results to the A4C Server through the A4C Client.

The AR functionality can thus be divided in three major areas:

1. **Quality of Service**

The COPS Attendant is the main interface of the AR. It is through this interface that the AR communicates with the QoS Broker. QoS requests from the mobile terminal will be translated into COPS messages and then delivered to the QoS Broker. QoS requests may come in the form of explicit RSVP messages or DSCP packet marking; whatever the case, and assuming that the AR is properly configured to handle those options, the AR will process them and deliver the appropriate COPS message to the QoS Broker.

The translation of external QoS signalling (IntServ for example) into internal DiffServ signalling, appropriate for the CN, is done by the QoS Manager module. This translation is then sent to the QoS Broker, where it is validated and communicated to the remainder of the network. Having the AR do the translations and the QoSB the validations and communications allows the distribution of processing effort among AR's and QoSB's.

If required, SIP requests are intercepted by the AR's Advanced Functions module and they are processed, else they are simply forwarded to the SIP Proxy. Processing of SIP messages is done to allow the extraction of relevant QoS information or even change the messages themselves.

2. **Access control**

The AR resides on an Access Network at the edge of the Akogrimo network, and thus, any attempt to unlawfully use network resources without proper permission will be halted at the AR.

A user is required to authenticate himself to the provider before he can use any resource of a provider's network. User authentication requests are intercepted by the AR and then forwarded to the A4C Server.

A user is immediately authorized once he has successfully authenticated. That authorization allows him to use basic network resources such as moving between different AN's.

When an authenticated user requests services from the network, it also has to be authorized before being able to use those services or resources. The authorization depends on the identity of the user, whether he has permissions or not to use that specific service, or also on the services which were previously subscribed by the user.

3. **Metering**

The metering module is able to do per-flow metering. Its results are communicated to the A4C Server, which uses them as a basis for accounting.

2.4.1.1. Access Router Interfaces

Component	WP	Purpose	Protocol
SIP Server	WP4.1	- Sending SIP requests	SIP
QoS Broker	WP4.1	- Receiving AR configurations - Sending resource requests - Sending mobility requests	COPS
Mobile Terminal	WP4.1	- Receiving resource requests - Receiving mobility requests - Receiving SIP requests	RSVP Mobile IPv6 SIP
A4C	WP4.2	- Sending authentication requests - Sending authorization requests - Sending accounting information	Diameter

Table 1 – Access Router Interfaces

2.4.2. QoS Broker

The QoS Broker is the network component which effectively manages all network resources. It receives global network policies from the PBNM system. Requests for QoS from access routers have to be approved by the QoS Broker which then sends appropriate configurations to the AR's. It also exchanges information with other QoS Brokers.

Mobility is also dependent on the QoS Broker, since a user may not change Access Network if, for example, the new AN has all its resources already occupied. When a user moves from an access network to another, both networks' QoS Brokers are involved in the process.

The QoS Broker architecture is depicted in Figure 7:

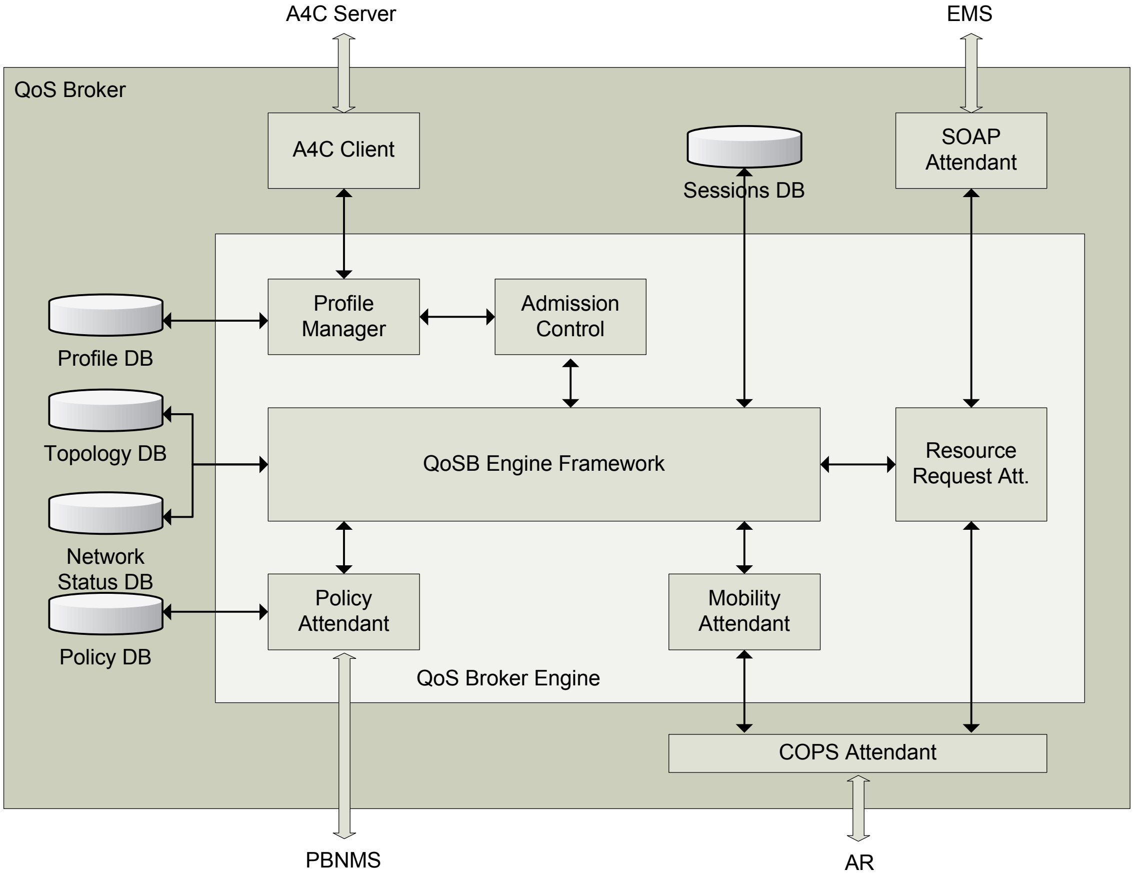

Figure 7 – Akogrimo QoS Broker

The QoS Broker has a Policy Attendant which communicates with the PBNMS and stores the policies it receives in a policy database. It is also possible for the QoS Broker to request policies by itself.

The COPS Attendant module allows it to communicate with the AR using the COPS protocol. It is through this interface that the QoS Broker will receive QoS requests and other information from the Access Routers. It will also be used to send appropriate configurations to the AR's.

The A4C Client allows the QoS Broker to retrieve user profiles from the A4C Server. Those profiles are then cached in the Profile database for efficiency reasons. This eliminates the need to do a request to the A4C Server each time the QoS Broker needs information from the user's profile.

A SOAP Attendant module is responsible for receiving QoS requests from the grid layer as well as sending the responses to those requests. QoS status notifications are also sent through this module to the EMS for SLA monitoring purposes.

The Topology, Network Status and Sessions databases are used for QoS Broker internal operation:

- Topology DB – holds information about routers and respective interfaces. It allows the QoSB to find an actual route for a data flow.
- Network Status – allows the evaluation of whether there are available network resources for establishing a new session.
- Sessions DB – holds information about ongoing sessions.

2.4.2.1. QoS Broker Interfaces

Component	WP	Purpose	Protocol
AR	WP4.1	- Sending AR configurations - Receiving resource requests - Receiving mobility requests	COPS
QoS Broker	WP4.1	- Receiving resource allocation requests - Sending resource allocation requests - Receiving mobility requests - Sending mobility requests	TCP
PBNM	WP4.1	- Sending policy requests - Receiving policies	CIM
A4C	WP4.2	- Sending user profile requests - Receiving user profile	Diameter
EMS	WP4.3	- Receiving resource availability requests - Receiving resource reservation requests - Sending QoS status change notifications	SOAP

Table 2 – QoS Broker Interfaces

2.4.3. SIP-related infrastructures

In order to provide commercial exploitation of SIP services some SIP related network infrastructures are needed, which are described from a functional point of view in RFC3261 [SIP01]. The basic set of these necessary entities are:

- The Location Service, or Location Database, which provides user location management to the domain it serves. It maintains a list of bindings of Address of Records keys (AoR: primary or default SIP address) to zero or more contact addresses (devices in which the user can be contacted), and must be accessible for the rest of the SIP network infrastructures.
- The Registrar Server, which accepts SIP REGISTER requests to update the information stored in the Location Database. Using the Registrar Server, users can update the information regarding their SIP location (where they can be contacted).
- One or several SIP proxies, whose primarily role is to send the request to the network entity closest to the user, so they are mainly used for routing. They can also rewrite specific parts of the messages before forwarding it (for example, change the AoR with the current contact address.

These basic infrastructures are depicted in the following figure:

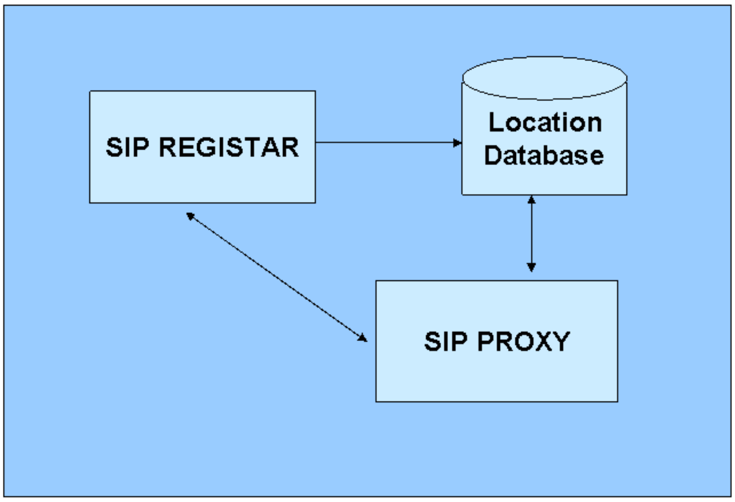

Figure 8 – SIP basic network infrastructures

It is possible to have these entities in different nodes, or co-located within the same one. Considering that both Location Database and Registrar are associated to a certain domain, it has sense to co-locate them in the same network node within the Core Network, so called the SIP Server. As it will need routing capabilities, it also includes a SIP proxy. So in principle we only need a SIP Server to provide SIP services in Akogrimo. Anyway, we can have SIP proxies for routing purposes in the access networks belonging to the same domain.

SIP can be used also to provide user presence and context information [SIP02]. This information has to be collected and delivered to the Context Manager, which is responsible to gather context information from many sources, not only SIP. We have included a subcomponent within the SIP Server capable of achieve this task, the Presence Agent (PA). .

Finally, in order to trigger grid-initiated SIP calls (see 7.2.2.1 and 7.2.2.2) a specialised SOAP/SIP-aware service has been envisaged. This service will receive a SOAP query from the grid layers with the information of the users to be put in contact and it will start a SIP process that will conclude with a call between them. In principle it could be possible to include it also in the SIP Server, but for scalability purposes, and to decouple SIP applications from basic infrastructures we decided not to include it in this component. In this process, the SIP Server only has to map AoR to the current contact address, so it will act only as a proxy.

Next subsections will describe these components and their interfaces in a more detailed way.

2.4.3.1. SIP Server description

The functional description of the Akogrimo SIP server is depicted in the following figure:

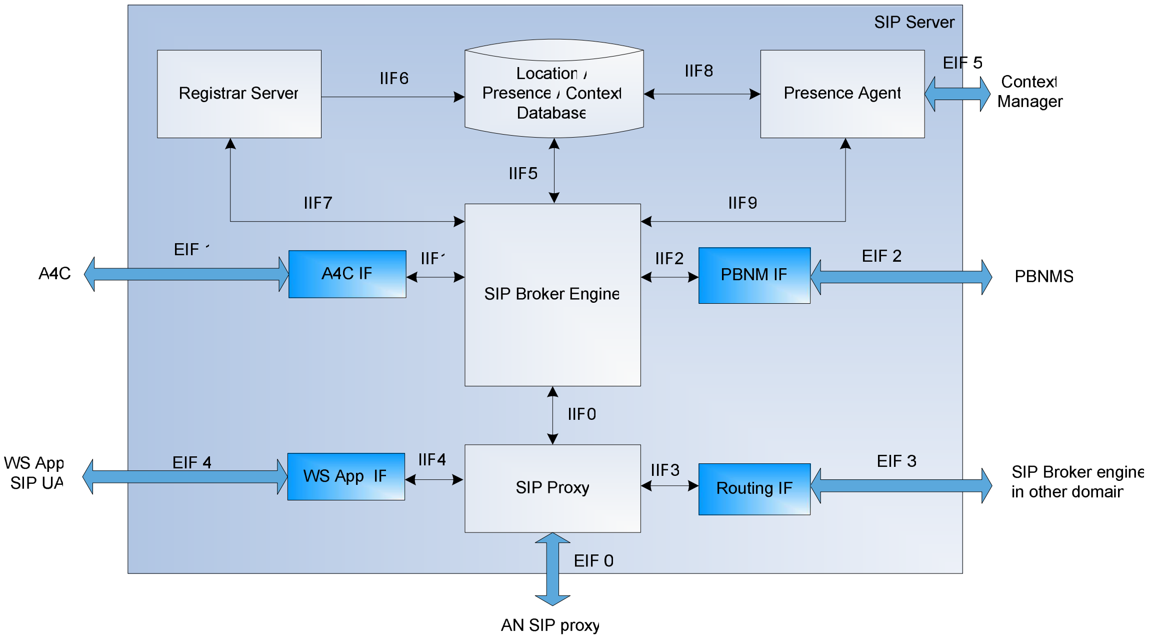

Figure 9 – Akogrimo SIP Server

The Registrar Server, Location Database and the SIP proxy are the functional entities that have been already described.

The SIP Server includes a SIP Presence Agent (WP42) in order to provide SIP-related presence/context information provided by the users to the Context Manager through a presence watcher interface (SIP SUBSCRIBE and NOTIFY). The presence/context status is stored in a database, which can be associated to the Location Database if we consider that the information it stores is part of the user context. In fact, the registration information could be useful to provide a "default user context" when there is no more information available.

The SIP Broker Engine is the core part of the SIP Server. It implements the interconnection logic between the different SIP entities as well as the interfaces with other network entities by means of the corresponding IF modules. Acting as the "brain" of the SIP Server, it takes decisions based on the nature and the content of all incoming requests. Only SIP routing capabilities are delegated to the SIP proxy, which will gather all SIP requests coming from users (through AN proxies, if any) and will pass them to the Broker Engine if it cannot process them directly. The Broker Engine analyses them and decides how to proceed.

2.4.3.2. SIP Server interfaces

Component	WP	Purpose	Protocol
AN SIP Proxy	WP41	Receive SIP requests and responses coming from the users. Send SIP request/responses to the users.	SIP
A4C	WP42	Request for user authentication and SIP Service authorisation. Parameters: AA token, service	Diameter

Component	WP	Purpose	Protocol
PBNMS	WP41	Receive policies related to SIP	CIM
SIP Server	WP41	Route SIP requests to a user in another domain.	SIP
WS Application SIP User Agent	WP44	Receive a request to put in contact two users. Parameters: AoR user 1, AoR user 2	SIP
Context Manager	WP42	Receive subscriptions to the SIP presence/context status of a user (receive SIP SUBSCRIBE requests from the Context Manager). Notify changes on the SIP presence/context status of a user (send SIP NOTIFY responses to the context manager).	SIP

Table 3 – SIP Server Interfaces

2.4.3.3. AN SIP Proxy description and interfaces

The architecture of the AN SIP proxies is very simple and depicted below.

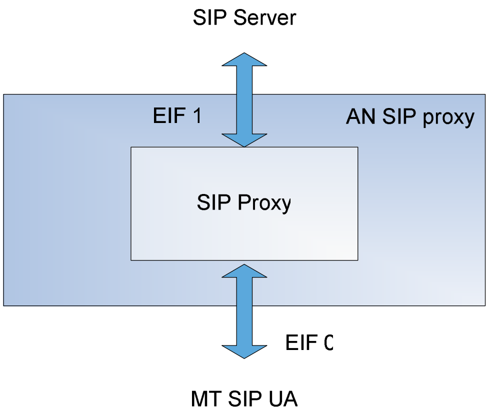

Figure 10 – Akogrimo AN SIP Proxy

The AN SIP proxy acts only as the intermediary between users in the AN it serves and the SIP Server. It routes all incoming SIP request and responses from the users to the SIP server and vice-versa without major processing. Only local responses (like a 180 "Trying" to an INVITE request) are automatically generated at this level. Both interfaces are standard SIP interfaces.

2.4.4. Home Agent

The Home Agent acts as home location registers for mobile terminals. This entity is a modified Mobile IPv6 Home Agent with appropriate interfaces for Akogrimo network control.

2.4.5. PBNM

Policy Based Network Management (PBNM) is an alternative for the management of telecommunications networks that offers a way of overcoming many of the limitations of existing human resource-intensive network management techniques. In heterogeneous and distributed environments like Akogrimo, network configuration to guarantee required end-to-end QoS, or to assure certain rules for admission or congestion control could be a very complex problem to solve without automatic mechanism for configuration and control.

The PBNM allows easy creation of policies through an intuitive interface and then applies those policies to all the machines affected. It will also respond to policies solicitations from entities which require them.

For more information regarding PBNM, please refer to section 6.

2.4.5.1. PBNMS Interfaces

Component	WP	Purpose	Protocol
QoS Broker	WP41	-Sending policy definitions -Receiving policy requests -Receiving policy-related information	CIM
SIP Server	WP41	-Sending policy definitions -Receiving policy requests -Receiving policy-related information	CIM
A4C	WP42	-Sending policy definitions -Receiving policy requests -Receiving policy-related information	CIM

Table 4 – PBNMS Interfaces

2.4.6. Mobile Terminal

2.4.6.1. Overview

The Mobile Terminal's operating system is Linux because of the need for Mobile IPv6. It will hold software modules from most Akogrimo work packages. They are presented in Figure 11:

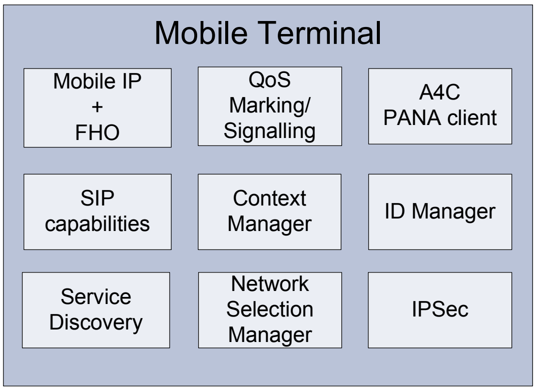

Figure 11 – Mobile Terminal software modules

The relevant modules for work package 4.1 are:

- Mobile IP and Fast Handover module – this module provides terminal mobility and seamless fast handovers which are essential for multimedia, audio or video usage in a mobile environment.
- QoS Marking and Signalling – this module enables the MT to perform QoS requests.
- SIP – provides SIP capabilities for audio/video conferencing and also session mobility to SIP-aware applications.
- Network Selection Manager – this module provides information on what network accesses there are available to the MT.
- IPSec – this module will provide secure communications; this is not considered in Akogrimo's first phase.

2.4.6.2. SIP Module

The following figure shows the SIP infrastructure in the Mobile Terminal.

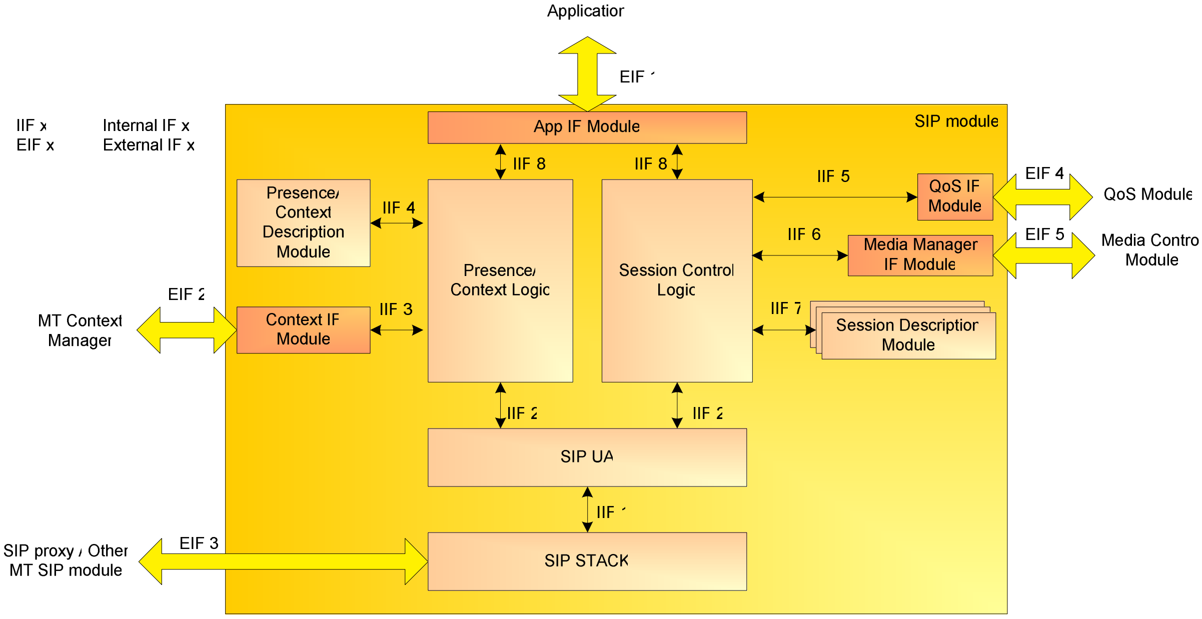

Figure 12 – MT SIP module

- **SIP Stack**: SIP Protocols stack (based on JAIN SIP).
- **SIP UA**: Low level handling of SIP messages and responses (overlaying JAIN SIP stack).
- **Session Control Logic**: this module is intended to control SIP sessions: setup, renegotiation, termination, transfer...Basically it coordinates all the needed interactions with other MT modules to effectively carry out these session handling activities. For example, if the application request for a SIP audio call setup, this module first extracts the corresponding QoS parameters associated to this communication and checks (through the QoSC interface) if there are available resources in the network. If yes, it requests the building of an appropriate SDP [SDP] file and will order the SIP UA to start the corresponding SIP session setup process.
- **Presence Context Logic (SIP PUA):** In charge of managing SIP enriched presence information. Converts it in a suitable format to MT Context Manager, which gathers all possible context sources. It implements only a SIP Presence User Agent (to publish presence/context information). In Akogrimo phase I users are not allowed to request context information, only services. When allowed, MT will request complete user context information through the MT Context Manager, and not using a SIP watcher. The reason is obvious: SIP context is only part of the user context, so it has no sense to know only the SIP part of the user context when the whole information is accessible. This is a WP42-related component.
- **Presence/Context Description Module**: this module parses the SIP-related presence/context information and generated the corresponding pidf/rpid body to be included in a PUBLISH message. This is a WP42-related component.
- **Context Manager IF Module:** is in charge of gathering context information, and when there is a user presence status change (busy, available, in conversation….) the MT send a SIP message to the SIP Presence Agent (which resides into the SIP Proxy), in order to update the presence information. This is a bidirectional API for publishing SIP based presence/context information. This is a WP42-related component.
- **Session Description Module (SDP):** This module is in charge of providing SDP to the SIP UA, in order to add it into the SIP message. Besides of this, is able to split in several parameters the SDP sent it from SIP UA and provide these parameters to the Application.

  The purpose of SDP is to convey information enough about media streams in multimedia sessions to allow the recipients of a session description to participate in the session. SDP is sufficiently general that it can describe conferences in many network environments.

  Basically the SDP includes: the session name and purpose, the time during the session is active, the media comprising the session, information to receive those media (addresses, ports, formats and so on). As resources necessary to participate in a session may be limited, some additional information may also be desirable, such as, information about bandwidth to be used by the conference.
- **Media Manager IF Module:** this module is responsible for real time traffic control over Real Time Protocol (RTP) [RTP].
- **QoS IF Module:** is in charge of requesting QoS information (for instance, bandwidth information), resources availability, or be informed about QoS related events. QoS related interactions will invoke network components so this will be an asynchronous interface.
- **App IF Module:** this is the interface between the end user application and the SIP module. It is a bidirectional interface to enable session control from end user application. For instance application will be informed that an incoming session has arrived, to decide if the session is accepted or not. Accordingly, this interface will provide methods to application in order to

terminate ongoing sessions. This interface will be used also to provide some needed parameters from other modules that have no direct interfaces with the SIP module. For example, the A4C_Token (to be included in all SIP REGISTRAR and INVITE requests to guarantee that only authorised users can make use of Akogrimo SIP infrastructure) will be provided using the application interface.

Apart from the presence-related functionalities, which are under the scope of WP42 scope, the main SIP-related tasks which are controlled by the Mobile Terminal are registration, session setup, the session transfer and the session termination.

When the Akogrimo user wants to establish a SIP session with other user, the first have to do is registration. Only authenticated Akogrimo users will be registered, that is, only authenticated/authorised users will make use of Akogrimo SIP infrastructures. Therefore the Registration process should be part of the terminal power on, and must take place after network registration.

Once the user is registered into SIP infrastructure, he can begin SIP session setup. As mentioned, the module "Session Control Logic" is in charge of the coordination of this task, that is, is in charge of gathering information related QoS (resources availability, bandwidth..) from "QoS Module", information related SDP from "SDP module", and after this transfer them to "SIP UA Module" in order to it build SIP message. Once SIP UA has built the SIP message it sends it to the closest SIP Proxy in order to continue the session setup process and if is a successfully process then the "session Control Logic" orders to "Media Manager Module" establish a communication (data flow over RTP).

Similar interactions will take place to renegotiate, transfer or terminate a session. In all cases, Session Control Logic is responsible for the coordination between MT submodules.

2.4.6.3. Media Control Manager

This module is responsible for the RTP traffic control. It is controlled by the SIP module to initiate, modify and terminate SIP sessions. Its structure is very simple:

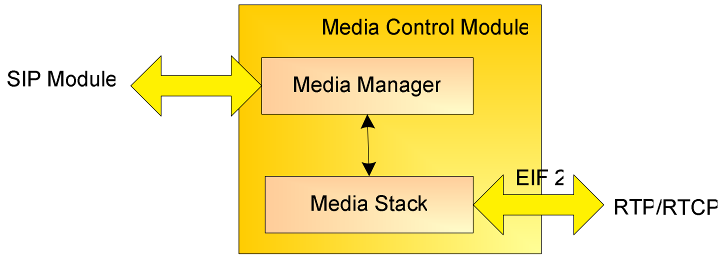

Figure 13 – MT Media Control module

The Media Manager submodule overlays an RTP media stack by offering an API to the SIP module in order to provide session control.

2.5. Interactions with other layers

2.5.1. Web Services interfaces

In the first phase of the project the network layer will expose some of its functionality as Web Services which will be easily accessible by higher layer components.

The SIP Server will allow grid initiated SIP calls (see 7.2.2.1 and 7.2.2.2) through a web service interface. The QoS Broker will also have a web service interface for both accepting QoS requests and for reporting QoS status to the EMS component (of work package 4.3) for SLA monitoring purposes.

2.5.2. 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. The application, even though it has the right packets, must discard them instead of reproducing 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.
- **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 5 shows the proposed QoS bundles for Akogrimo.

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

Table 5 – QoS Bundles

Should these bundles prove insufficient or inadequate, they can be easily modified or new ones created.

A bundle is applied to a specific flow. The user may use several bundles at a time, applied to different flows provided that his contract allows it. If a running application requires changes in the QoS bundles, this can be done by making a request for a new bundle.

3. Mobile Access Infrastructure

3.1. Introduction

Mobility, as previously shown, is an essential pre-requisite for Akogrimo. This chapter presents a solution that allows seamless, transparent mobility, independently of the underlying access technology.

This solution must support a common way for a network to manage end-users, regardless of the specific access technology they are using, and while in doing so, it must also support seamless mobility in a transparent way to higher layers. Performance is also essential, for disruptions during mobility handovers should be eliminated or kept to a minimum.

3.2. Terminal Mobility

3.2.1. Mobile IPv6

A network which is supposed to be ubiquitous and allow any kind of heterogeneous nodes can not be linked to one single access technology. It is worth mentioning that seamless mobility between different access technologies has been previously achieved in the Moby Dick project and is being deeper studied in the Daidalos project. The base to permit this link-layer independent mobility is given by Mobile IPv6 [MIPv6], which is a network layer mobility solution based on IPv6 [IPv6].

This is by no means an attempt at fully explaining Mobile IPv6 – other documents have done this quite well. However a very short description, either for introducing basic concepts or remembering forgotten ones, was deemed desirable.

3.2.1.1. Basic Functionality

Due to the fast evolution and constant growth of the Internet, there has been a need to redesign IPv4 in order to accommodate present and future demands. To this end, IPv6 was developed as a replacement of IPv4. It brings along a lot of improvements to IPv4; among others, extended addressing capabilities, header simplification, extensibility, etc… However, for both IPv4 and IPv6, the IP address topology is designed in a way that determined addresses belong to determined networks or sub-networks, and thus, the routing of packets is performed according to this structure. If a node disconnects from its point of attachment to the network and connects to the network at any other place, a reconfiguration of a new IP address, netmask and routers is necessary. Mobile IPv6 extends IPv6 so that mobile terminals are able to change their point of attachment to the network with minimal disruption. When a mobile terminal roams across different networks, Mobile IPv6 deploys a mechanism, restricted to the network layer that makes this change of position in the network transparent to higher layers. Therefore, already established connections (for example a TCP connections) are not dropped when a node changes its position from one network to another and needs to reconfigure its network characteristics. In fact, these connections are not even aware of this change. Since Mobile IPv6's scope is restricted to the network layer, it does not impose any requirements on the lower layers. This means that a mobile terminal is able to roam across networks independently of the access technology. For example, a hand-over may take place between two Ethernet accesses or between an Ethernet and a WLAN access without any concern.

The main idea of how mobility has been implemented in MIPv6 revolves around the use of not only one but two addresses for a node to be exhaustively addressable at any point. Theses addresses are:

- Home Address (HoA): As any other regular node, a mobile terminal has a permanent address, which is valid inside his home network. This address always remains the same, independently of in which network the mobile terminal is located, i.e. whether at home or roaming. This is the only address that the transport or higher layers are aware of.
- Care-of Address (CoA): For as long as the mobile terminal is located in a network other than its home network (i.e. a foreign network) it makes use of the CoA, which is a suitable address for the foreign network in which the mobile terminal is located at that moment. The relation between the HoA and the CoA of a mobile terminal is called binding.

The new entities that the Mobile IPv6 protocol adds to IPv6 are described as follows:

- Mobile terminal (MT): A node with the ability to change its point of attachment to the network keeping connections alive.
- Home agent (HA): A node that resides at the MT's home network, which is in charge of forwarding traffic directed to the MT while it is away from home so that it looks as though the MT is virtually at his home network. To this end, the HA must be aware of the MT's current binding.
- Correspondent node (CN): Any peer node which a MT is communicating with. A CN does not necessarily have to implement mobility i.e., a CN may be either mobile or stationary.

When the MT is away from his home network the HA will act on behalf of it forwarding all the packets addressed to the MT at its HoA to its current CoA by means of a tunnel. The CN is not aware that the MT is roaming unless it supports Mobile IPv6. If this is the case, the CN will realize that its traffic is being tunnelled by the HA and may perform a route optimization by directly communicating with the MT by means of the MT's CoA instead of using the tunnel provided by the HA. This last should be the standard mechanism because it notably increases the performance. In order for the MT to communicate its position to the HA and all the CNs it is communicating with, a procedure is launched in which a packet called Binding Update (BU) is sent with the address currently used and a packet called Binding Acknowledgement (BA) is received by the MT as a confirmation. Regarding security, these packets should be protected, since several attacks can be applied if this is not done (man-in-the-middle, impersonation, DoS and others). The standard way to protect these packets is IPSec although there are other alternatives, such as using cryptographically protected CoAs.

3.2.2. Fast Handover

The goal of Mobile IPv6 is to achieve seamless mobility of devices. Due to its movement, the MT may have to change its point of attachment to the network by using a new access router that is closer to its current position. This change of point of attachment to the network is called handover and involves acquiring a new CoA and communicating the HA and CNs its new location before it can be fully operative again and the communication can be re-established. Voice applications, for example, are very sensitive to delays and need the handover to be fast enough in order to for it to be seamless.

Fast Handover reduces handover latency by anticipating the handover by means of the link layer. It allows the MT to start sending packets on a new network link as soon as it is detected, and also allows the MT to receive packets as soon as its attachment to the new link is detected. This way, while maintaining the previous connection intact and sending packets through it, the MT also sends packets through the new network link (effectively duplicating the packets). This avoids the loss of packets during the handover process and consequent degrading of quality in applications that are making use of the network.

3.3. Mobility Infrastructure

3.3.1. Mobility management entities

The active participants in terminal mobility are

- Mobile Terminal
- Access Router
- Home Agent
- QoS Broker

The MT, AR and HA are a necessity of Mobile IPv6 by definition. The MT needs to connect to the network using the AR's, and it is the HA which keeps track of the "real" location of the MT.

Mobility in Akogrimo will also be dependant of the QoS Broker, since for handovers to occur successfully without disrupting ongoing sessions, it is necessary that the QoS Broker checks that the handover can indeed take place.

If MT is connected (in AN1) through AR1 and moves to AN2, a handover process is initiated. AR1 informs QoSB1 of the MT request to handover. QoSB1 by itself may not make an informed decision, for it does not know the current state of AN2, so it contacts QoSB2 and informs it that a handover is to take place. It also presents QoSB2 with information regarding current MT sessions. QoSB2 can then verify if its AN2 can hold the MT sessions; if it cannot, it tells QoSB1 that the handover is not possible. If the handover is possible, then QoSB2 sends its response to QoSB1 and also sends a message to AR2 informing it that the handover is permitted. QoSB1 also tells AR1 that the handover was authorized and the handover is performed.

Section 5.3.5 depicts a message sequence diagram of a successful handover and presents its explanation.

This whole handover manoeuvre may introduce vulnerabilities that should not be overlooked. Section 4.3.2 explains what countermeasures can be used to palliate them.

3.3.2. Mobility scenarios

There are two major scenarios in terminal mobility regarding how it is decided whether the MT is to perform a handover or not.

The most usual scenario is Mobile Terminal Initiated Handover (MTIHO); it is initiated by the MT when, after detecting the presence of a new AN, it verifies that its signal is stronger and is thus beneficial to move to the new AN.

The other scenario, which will not be considered for Akogrimo, is Network Initiated Handover (NIHO). In this case, the network itself has load-balancing mechanisms that detect heavily loaded access routers. If a MT is reachable through another, less loaded AR, then the network initiates a handover procedure in order to move the MT to the less loaded AR.

4. Network Security

4.1. Introduction

Security in networks is per se mandatory in any network architecture nowadays since in most cases personal, confidential or simply important data is transmitted through them and exposed to malicious third parties. One of the most important values of Akogrimo is mobility. Mobility implies roaming nodes using different networks that they may not know anything about and no decision as to whether they can be trusted or not can be made. Furthermore, the fact that by default the kind of networks used for mobility are wireless makes it easier for an unknown third party to tap the connection, tamper information or perform any other attack (e.g. Denial-of-Service (DoS) attack). In addition, the necessity of security is increased even more when we realize that one this project's most important targets is to make Grid networks be used with commercial purposes that involves the issue of contracts and agreements among the interested commercial partners. Akogrimo will develop the necessary security infrastructures to provide privacy, authenticity, integrity and non-repudiation as an inherent part of the overall project. In order to develop a solid integrated security model involving the different layers of the Akogrimo stack, security will be considered in depth in the second iteration of the project, due to the fact that security standards in the Grid community are still under early development and therefore change rapidly, are fast evolving and have not yet reached a stable goal.

4.2. Identity & Authentication

Identity and Authentication are two closely related issues that are handled mostly in the WP4.2. After having studied these aspects more in depth, it has become clear that a much better development will be possible reallocating these efforts into WP4.2. The rationale for this is that a much better integration between Networks and Grid services can be achieved if identity and authentication in networks are treated with the same basis as in Grid services and not as something developed independently from each other that is linked later. By doing this, in addition to have a better integration, an easier management of these concepts is possible. As it was stated before, the WP4.2 was in charge of development of the AAA Diameter [AAA][DIAM] structure, whereas WP4.1 was in charge of the authentication of the user by means of the PANA protocol [PANA], which conveys the necessary authentication information to the AAA and the other way around. For the sake of simplicity, clarity, integration and productivity these efforts will be reallocated in WP4.2.

4.3. IPsec

Among all the security issues that have to be handled one of them is to provide security in the communications between nodes. Considering that this project aims to build an all-IP based beyond-3G network, a uniform system to secure communications has to be provided independent of the security provided in the underlying L2, since any access medium can be utilized (WLAN, UMTS, Bluetooth…) and the security methods provided by each one of them are different. In order to homogeneously protect the communications that take place security in a layer above L2 must be provided. IPsec [IPSEC] is considered the standard security protocol for IPv6. It works at network layer and provides encryption and authentication for IP packets, in a total transparent fashion for the upper layers. Other solutions exist to provide security in higher layers but in our case they would be a complement to IPsec. For instance, SSL/TLS (Secure Sockets Layer/Transport Layer Security) provides secure communications working, however it imposes restrictions on the type of traffic carried, e.g. it doesn't support the protection of UDP traffic.

IPsec is a very versatile protocol that can be utilized for different purposes. It works in two different modes, tunnel and transport. Transport mode secures the packet's payload and is suitable for E2E secure communications; on the other hand, tunnel mode capsules the whole packet, including headers, and is typically used to establish virtual private networks connecting two different networks or a single user to the private network. IPsec requires an authentication and negotiation of the security mechanism to be used before the communication takes place. This is done using a protocol called Internet Key Protocol (IKE) [IKE]. In the wireless scenario that is mostly dealt with in Akogrimo, the connection between the MT and access network is especially important. Independent of the underlying access media used, IPsec will provide secure access to the core of the Akogrimo network by means of an IPsec tunnel between the Mobile Terminal (MT) and the Access Router (AR). After the MT and the access network authenticate towards each other making use of the PANA and Diameter protocols, some cryptographic material is conveyed through the A4C structure to the AR and the MT. By means of the IKE protocol and the cryptographic material distributed by the A4C, MT and AR can authenticate each other and afterwards establish an IPsec SA (Security Association), cf. Figure 14.

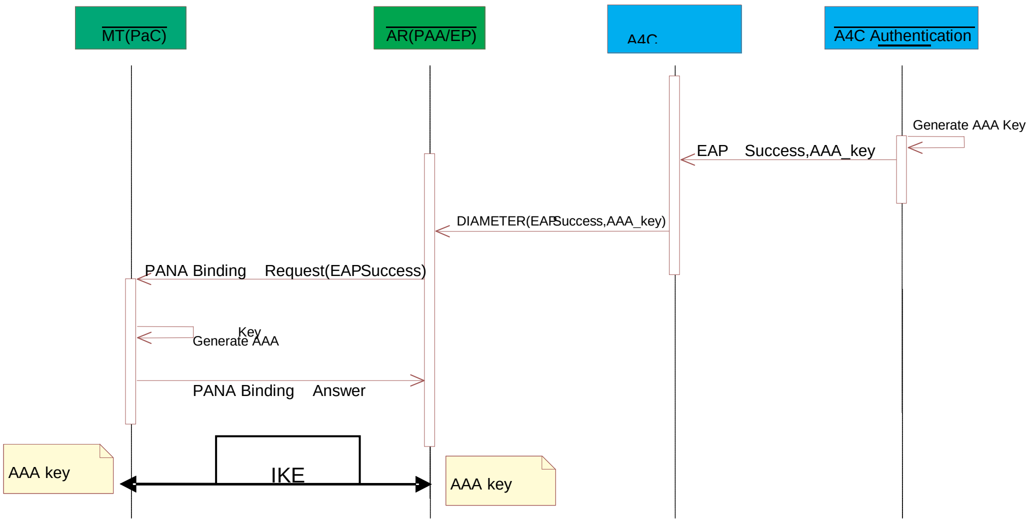

Figure 14 – IPsec key distribution after authentication

The core of the network is considered to be secure to a certain extent and therefore, as a general rule, E2E security mechanisms are considered advisable, but not mandatory, unless the necessity to protect the data is obvious (identities, transactions, and so forth). To this end, additional methods such as IPsec in transport mode, SSL/TLS or OpenPGP can be used to complement IPsec.

4.3.1. IPsec peer authentication

IPsec is used to provide secure communications between two hosts, typically using the addresses of the hosts involved as an identifier for the authentication (IKE phase 1), which needs to take place between the two hosts before negotiating the type of secure communication to be build (IKE phase 2). The fact of using an IP address as identifier of the nodes forces a device-centric approach of IPsec. This project focuses much more on users working with more than one device, or that want to, as transparent as possible, move a session from one device to the other. It would be a total waste of resources to build a sophisticated identity management system on the overall project whereas communication's security associations are based on device IP addresses. Fortunately, identifying the peers that want to establish a secure communication by more than just the IP address is possible with IPsec. User FQDN (Fully Qualified Domain Name), USER_FQDN, KEY_ID or ASN.1 distinguished names are possible identifiers that could be used. IPsec backed by a strong Identity Management structure will consolidate an overall secure communication platform and ensure the use of cryptography in an intelligent way, since there is no worse security breach than the false sensation of security.

Several types of authentication are possible with IKE: shared keys, certificates or public-private keys. These authentication methods are not exclusive from each other in the meaning that a certain user can use different methods depending who he is communicating with. We identify that some methods are more suitable for determined situations and therefore different types of authentication methods are envisaged in this project. For the case in which a user arrives to a new network, proves its identity with the A4C structure and then gets access to the network by means of an IPsec tunnel between his terminal and the AR, it seems most suitable to use a session shared key that is distributed using the authentication messages in order to save round trips and therefore commit the overall process of access to the network as fast as possible. This is of especially importance since a roaming user would otherwise notice that a handover took place or even established connections could break down. In the case of two peers that want to establish a spontaneous point to point secure communication without knowing anything from each other, a method such as certificate-based authentication would fit better the needs of the situation.

4.3.2. IPsec and MIPv6

Especially important is to secure MIPv6 with IPsec so that the introduction of this kind of mobility mechanism does not imply extra vulnerabilities compared to regular IPv6. Therefore, Binding Updates (BU) and Binding Acknowledgements (BA) MIPv6 packets will need to be protected. The fact that a node may perform a handover from one AR to another also implies the need to build a structure to enable the different ARs involved the sharing of SAs. That way, the handover takes place with maximum celerity and therefore remains seamless.

4.3.3. Existing IPsec implementations

The linux implementations of IPsec are divided in two parts: a kernel part, which makes most of the work, and a user space program in order to configure it and negotiate encryption keys. Regarding the kernel part, the linux 2.6 kernel comes with an IPsec stack provided by the KAME project [KAME]. An alternative to this implementation comes by the hand of the Openswan project [SWAN]. These projects also provide the necessary user space tools. Due to the adoption of the KAME IPsec implementation by the kernel's main line it seems to be the most promising implementation to use.

5. Quality of Service

5.1. Introduction

Quality of service can be defined in a very basic sense as consistent and predictable delivery of data. The Akogrimo network must be able to provide such diverse services as interactive audio (e.g. a SIP audio session) or large data transfers (e.g. some Grid service which requires large portions of data to be transferred among different machines for computation). These diverse services have completely different requirements on a network level. The former requires a relatively small amount of bandwidth (e.g. 64Kbps) but very strict latency requirements, in order to allow a normal conversation without interruptions. The latter requires large amounts of bandwidth (e.g. 512Kbps or more) but is tolerant when it comes to latency, since a delay does not affect the computation of the data. Quality of service is used in this case to accommodate the different network flows according to their requirements and at the same time optimize the use of the network resources. QoS also has an impact on the reduction of network infrastructure costs.

For the Akogrimo project it was deemed necessary the creation of Web Service interfaces using the SOAP protocol for allowing grid layers to perform QoS reservations. So, in addition to the network layer signalling methods there will be an interface designed specifically for interaction with the grid layers.

This section will present the functioning of the QoS system and the interactions among the major components involved in QoS (Access Router and QoS Broker).

5.2. QoS signalling

5.2.1. Network layer QoS signalling

Network layer QoS signalling will be used by network layer components for performing QoS operations.

For making QoS reservations, some kind of signalling has to be implemented, in order to inform the QoS Broker of who is asking for a reservation, and what the reservation is. So as to provide some flexibility and even support for legacy, non-Akogrimo ready applications, different signalling mechanisms need to be in place.

Since it is the AR's which receive requests from user's terminals, it is logical that the AR's that be the ones that support those different mechanisms. The QoSB will always receive COPS messages, independently of the reservation mechanism used initially. The AR is responsible for recognizing, processing, translating reservations made using whatever mechanism into COPS and finally sending them to the QoSB.

The reservation mechanisms that will be supported are:

- DSCP – the AR is capable of detecting the DSCP of a specific flow and, given appropriate configurations to handle the flow, treat it according to what was specified. This is of particular importance for legacy application support, which is not prepared to use explicit RSVP signalling.

- RSVP – this is the preferred method for Akogrimo-ready applications. The use of this explicit signalling method offers more flexibility to the application

- SIP – this method will be able to extract relevant QoS information from SIP messages and also of changing the messages. It provides the operator with the ability to extend the information carried by the SIP message, filter messages or tune network parameters.
- Connection Tracking – this method is able to track TCP sessions. Used in conjunction with DSCP, it can relieve the user's terminal from having to mark correctly each packet by marking a specific TCP session with an appropriate DSCP code.

In the first phase of Akogrimo only DSCP and RSVP will be considered. An application, such as a SIP enabled application, may use any of these methods for performing QoS reservations. If the application does not use RSVP, then the AR's have to be configured to recognize the application's packet flow so that the AR's may take the necessary steps for providing it with the QoS that is required. If the application has RSVP capabilities it may use RSVP and take advantage of enhanced flexibility. The application itself will request the QoS it desires and send RSVP messages to the AR.

5.2.2. Web Service based QoS signalling

One other possibility for requesting QoS is the use of a Web Service interface. This solution is aimed at grid-layer applications, and it enables any grid layer application to not have to know any details about the network layer. In this case the request is received directly by the QoSB, i.e. there is no AR interaction in the setting up of the QoS. After performing the necessary validations, the QoSB configures the affected AR's appropriately.

5.3. Interactions

5.3.1. Authentication and authorization

Before a user can use any resource of a provider's network, he is required to authenticate himself to the provider. The process of user authentication binds the user with an identifier. This identifier will then be used in any future interaction between the user and the provider.

A user which is not registered will not be allowed to communicate with the network except for requesting its authentication. Upon successful authentication, it will then be allowed access to the network.

The messages requesting a user's authentication must be caught as soon as possible, in order to avoid possible security risks. They will be caught by the Access Router's PANA Attendant module. The Access Router (AR) resides on an Access Network at the edges of the network, and thus, any attempt to exploit weaknesses in the authentication process will be halted at the AR. Also, there will be at least one AR responsible for each one of the provider's Access Networks (AN).

Figure 15 shows the messages exchanged between the various parties involved in the authentication and initial authorization process.

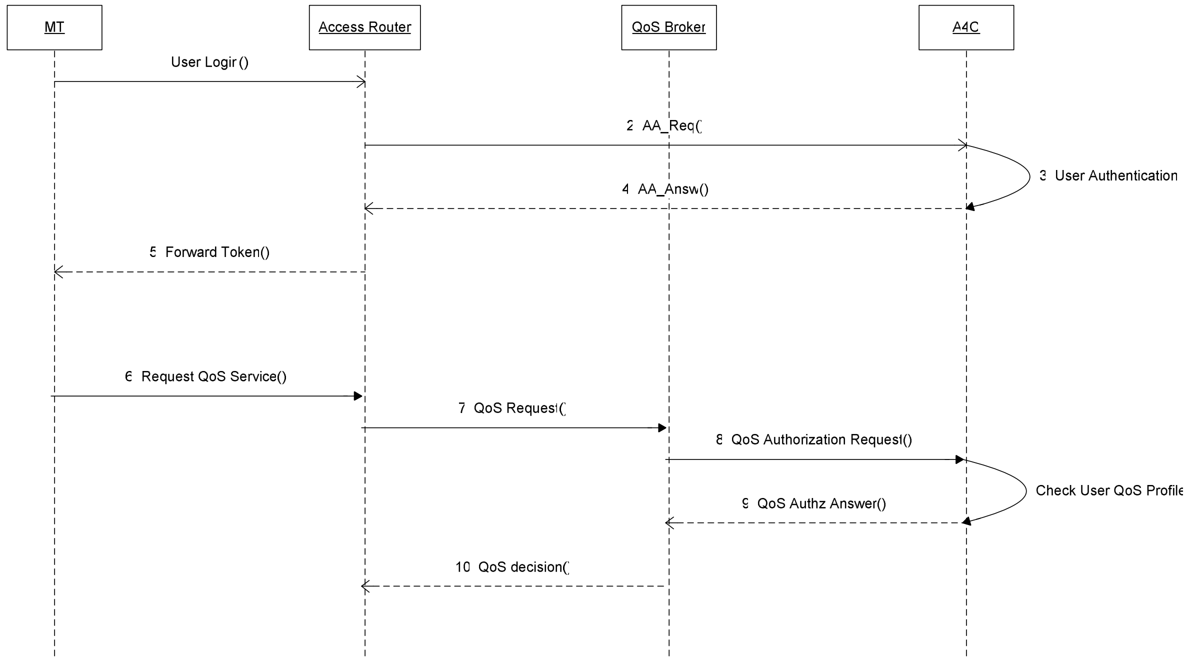

Figure 15 – Authentication and initial network authorization

First, the user requests that it be registered in the network. To that end, it sends a message (1) to the network with its identifier. That message will be caught by the AR's PANA Attendant, which will forward the message to the A4C server (2). The A4C server then verifies the authentication request (3) and answers whether it was successful or not (4) to the AR. Along with the answer follows an identifier (e.g. a SAML artefact) which will be used for identifying the user in future transactions. Finally the AR forwards the response (5) to the user. The authorization is explicit: the user request a QoS connection (either within the first message (user login) or separately later on with the QoS request) and the AR queries the QoS broker with the QoS Request (e.g. it can be a COPS request) whether the QoS connection can be provided. The QoS broker, in turn, requests the QoS authorization from the A4C server.

The communication between the user terminal and the AR will use PANA to carry the authentication protocol EAP, whereas messages between the AR and A4C use Diameter.

A successful authentication binds the user identifier to an interaction identifier. This binding will last until the user de-registers itself from the network. De-registration may happen due to user explicit request or due to a time-out. Upon a successful authentication, the user will establish a Security Association (SA) with the AN so that future communications are done in a secure fashion using IPSec.

5.3.2. User Authorization

When an authenticated user requests services from the network, it has to be authorized before being able to use those services or resources. Authentication and Authorization are separate processes. The authorization may depend on the identity of the user, whether he has permissions or not, or also on the services which were previously subscribed by the user.

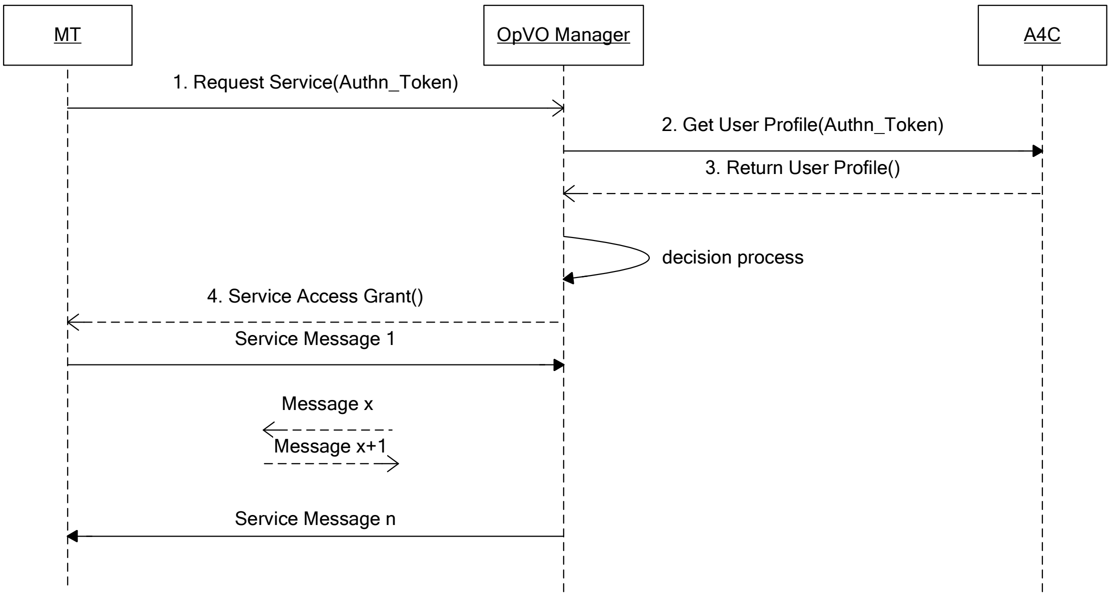

Figure 16 – User Authorization

Figure 16 shows the messages exchanged between each one of the elements involved.

The user requesting the service sends a message to the OpVO Manager (1). The OpVO Manager has to check if the user is authorized, so it requests the user profile to the A4C Server (2, 3). Taking this into account, it then decides whether to grant access to the user and responds accordingly (4).

5.3.3. Generic QoS Request

Setting up QoS involves having the user's terminal request network resources to the AR. The AR then communicates with the QoS Broker which will determine if the requested resources are available. If the QoS Broker doesn't have enough information about the user, it will need to contact the A4C server in order to get an authorization for the user and the resources which were requested by the user.

Figure 17 shows the message exchange during the QoS setup. Note that possible messages from the QoS Broker to the A4C server for performing authorization were omitted.

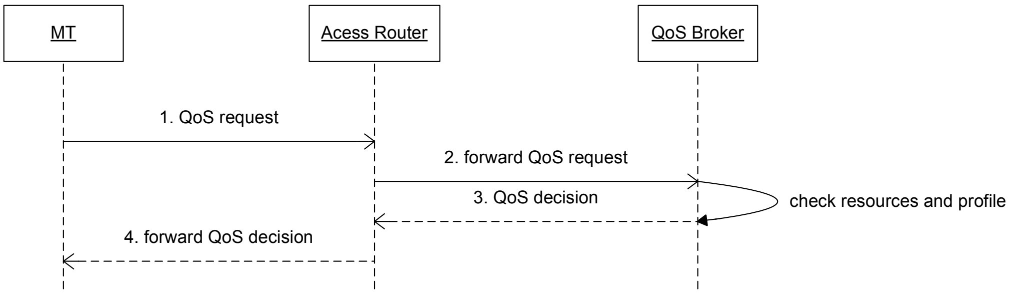

Figure 17 – QoS setup

Here we can see that the user is requesting some resources (1) to the AR, which forwards that request to the QoSB (2). The QoSB decides whether the user is authorized or not and whether it has the right to use the requested resources. The decision is then transmitted to the AR (3) and finally to the user (4) which had performed the initial request.

Note that this MSC depicts only one QoS request. In practice, a normal QoS request implies two reservations: one for upstream and another for downstream. For example, when user A starts a SIP telephony application and makes a call to his friend user B, QoS reservations must be made for the flow from A to B and also from B to A.

5.3.4. Web Service based QoS Request

Setting up QoS through the Web Service is done in a different way. In this case, the QoS Broker receives the requests not from the access routers, but directly from the EMS.

Figure 18 shows the message exchange during the QoS setup. Note that possible messages from the QoS Broker to the A4C server for performing authorization were omitted.

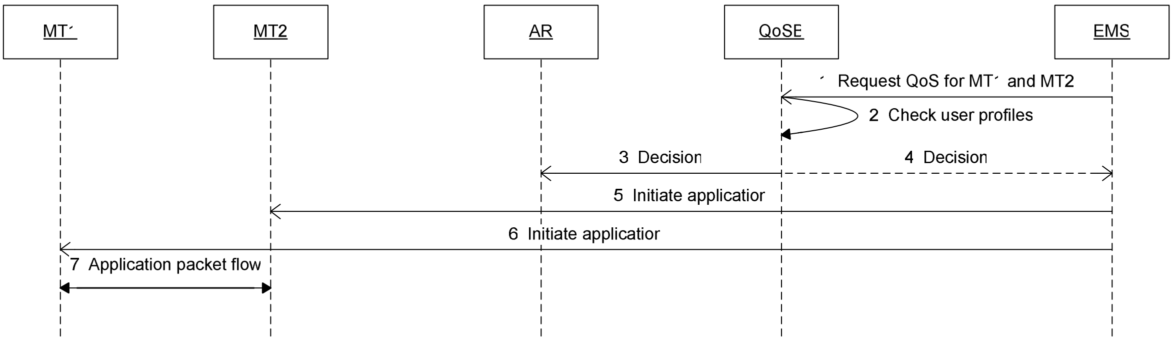

Figure 18 – WS QoS setup

In step (1) the EMS requests a QoS reservation for use by two Akogrimo users. The QoSB checks the users' profiles to verify that it is indeed possible for them to have that reservation (2) and sends its decision to the AR (3), so that it can configure itself for the upcoming QoS session, and the EMS (4). The EMS can then signal both users' applications that they can start (5, 6). Step (7) shows the application packet flow between both users.

5.3.5. Mobile IPv6 Handover

Maintaining QoS in a mobile scenario requires great coordination between QoS and Mobility elements.

When a MT decides to move from a network to another, it must inform (1) the old network AR that it is going to move to a new network. The AR sends a COPS message to the old network QoSB (2) asking whether the handover should be allowed or not. Since the handover involves one other QoSB, the old network QoSB cannot make a decision by itself. Hence, it sends a message to the new network QoSB (3) containing information about the user and his current sessions. The new network QoSB then decides if it has available resources to meet the MT's requirements and if the handover may be performed. If that's not the case, a renegotiation and/or adaptation of QoS is necessary.

This whole process must be extremely fast, so as to allow seamless handovers.

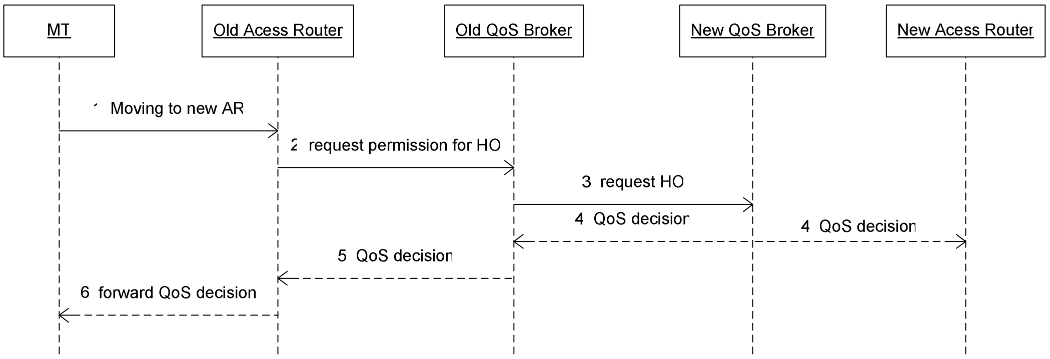

Figure 19 – Performing a handover with QoS

After making the decision, the new QoSB sends the decision to the old QoSB and also to the new AR (4), so that preparations for the handover may be initiated promptly. The old QoSB transmits the decision to the old AR (5), and the old AR transmits it to the user terminal (6).

6. Policy Based Network Management

6.1. Introduction

Modern networks can be very large and very complex to maintain. A Policy Based Network Management system aims to alleviate the burden of network administrators by presenting the administrator with a simplified set of more human friendly rules which he can manage more easily. PBNM also provides the ability of actually enforcing those rules on network components in an automated way, minimising work that would be tedious, laborious and error-prone for humans.

This chapter presents the PBNM system and its interactions with the main network components.

6.2. PBNM Architecture

The PBNM Architecture consists of a central (per-domain) server – the policy manager (PM), a database storing the rules and various interfaces to other entities in the network infrastructure. Most of these components use different protocols to communicate. Therefore, for each entity there is a translator module, which translates between the PM using CIM and the protocol of the corresponding entity.

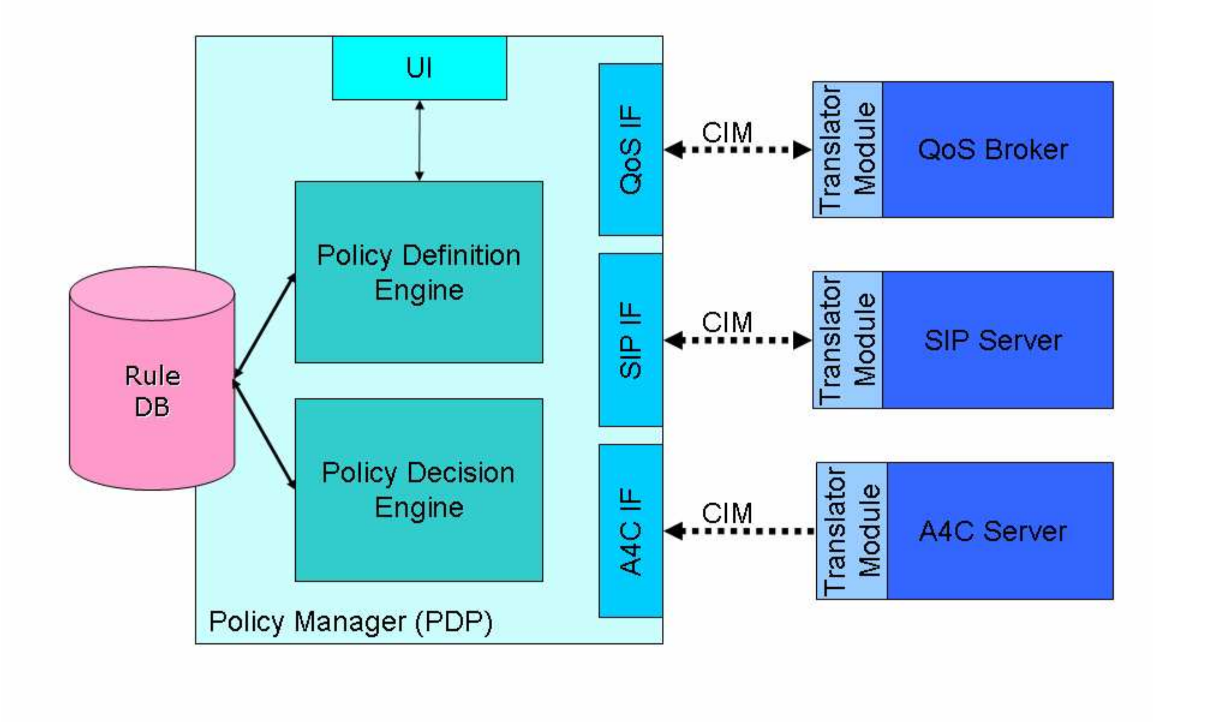

Figure 20 – PBNMS Architecture

These entities can be divided into two categories:

1. Information providing entities – these entities deliver some information based in which the policy manager chooses the appropriate rules. The different systems may differ in the actuality of information they provide, more static or more dynamic data.

2. Rule enforcement entities – these entities deploy the rules given by the policy manager.

Entities can belong to both categories at once, e.g. the QoS System has information about current number of users and streams inside the network, which could be used for the PM, and at the same time it enforces rules of the PM.

The following components are candidates for the first category, information providing:

- QoS System – the QoS system is capable of providing information about the current number of users in an access network as well as the number of streams per class, etc. This is quite dynamic information
- A4C System – the A4C system can provide information about what users are currently online, what services they prefer etc. which could be used to reconfigure the network to their special needs. This is more static information.
- SIP server – the SIP server can provide information about the current number of session manage in the network. It might also provide information about the demands of these sessions. This, again, is dynamic information.
- Monitoring system – A monitoring system can give additionally information about the users and streams in the network not only based on the requested reservations or sessions, but on their actual utilization of the network. (Out of scope for Akogrimo, we do not have a network monitoring system)
- Manual/ Time – it is also possible to choose rules manually or give times of usage for the rules.

These components can act as rule enforcement points:

- QoS system – the QoS system is the basic and most obvious entity to enforce the rules given by the PM. Rules can be the sort of changing available classes, reducing classes, allowing/denying access for terminals, etc.
- SIP server – The SIP server can also be used to deploy rules, e.g. initiate the renegotiation of sessions to change their QoS requirements.

6.2.1. Components of the policy manager

The policy manager consists of several components:

- Policy definition engine – The Policy definition engine converts the rules defined by the network operator (e.g. using a web interface) into a usable format to store. It also checks for concurrent rules. These rules then need a priority in order to allow deterministic network configuration.
- Policy decision engine – Policy decision engine is actually the heart of the PBNM system. It uses the information provided by the network to decide which of the rules currently have to be used.
- Interface modules – For each of the entities in the network that have to correspond with the PBNM system in one or another way, an interface module is needed to translate the rules into something useful for the entity (the correspondent or the PM, depending on the direction of this interface) as well as to translate the communication protocol if required.
- Database – the database is simply storing the rules of the PBNM system. Normal ways to access them is LDAP or SQL.

- User Interface – an Interface, e.g. a Web Interface, but also could be a Web Service, to define new rules, etc.

6.3. PBNM Rules

Given the above described architecture, there are many possibilities what rules to define. The following will show the groups along with some examples.

A rule generally consists of two parts:

- The first part is describing when a rule will be used:
    - User in the network
    - Flows in the network
    - Current QoS scheme
    - (SIP) sessions in the network and their requirements
    - Type of user (premium, standard, …)
    - Special requirements of a user
    - Time
    - IP-Addresses
    - …
- The second part describes what have to be done/reconfigured.
    - Change QoS scheme
    - Renegotiate SIP sessions
    - Prohibit special services (e.g. SIP video communications)
    - …

The second part also includes information about what type of entities to reconfigure, e.g. all routers, all SIP servers, etc. All combinations of the first and the second part are possible and correct rules, but not all make sense. Not only one basic rule(part) can be used, they also can be used to build complex rules using Boolean logic. Here are some examples for possible rules:

- Mark all packets from IP address x for QoS class y.
- If number of users in AN higher then x, change the QoS classes to y.
- If number of audio sessions (phone calls) is higher then x, renegotiate SIP session and reduce max. bandwidth to y
- If a premium user is inside the AN, change QoS scheme to allow a maximum bandwidth of x.
- During time span, allow free-of-charge low quality phone calls. (actually 2 rules, one to start and one to stop this)
- Or a complex one: If number of users is higher than x and there are no premium users connected, renegotiate SIP sessions to reduce max. bandwidth to y and prohibit video communications.

In addition to this, the rules contain one or more entity types which have to process this rule so the PBNMS knows to which entities the rule has to be sent.

6.4. Akogrimo PBNMS architecture

The Akogrimo PBNMS will be build up on the OpenWBEM (http://openwbem.org), an open source implementation of WBEM (Web Based Enterprise Management, http://www.dmtf.org/standards/wbem/). WBEM is an industry-driven approach to provide a set of standards and protocols for a unified management of systems, networks, etc. independent of vendor and/or environment.

openWBEM mainly provides a framework for management and monitoring. It is using CIM (Common Information Model, http://www.dmtf.org/standards/cim/) for communication with other entities.

6.4.1. Daidalos Extensions to CIM

Daidalos is developing some extensions to CIM in order to reflect the special needs of the involved systems. To find more details about Common Information Model refer to http://www.dmtf.org/standards/cim. You can find there the description of main CIM concepts like class, instance, dependency, core schema, common schema, extension schema etc.

The class definitions for Daidalos mainly include the entities “network” and “logical entity” as well as specifications for several services, whereof the QoS and A4C are from interest for Akogrimo. The specification can be found in “Daidalos CIM Extensions Whitepaper”.

6.4.2. Testbed Description

The current testbed consists of three entities, which are needed for the PBNMS:

- CIM Navigator (http://cimnavigator.com/) is a Java client application that can be used to graphically browse CIM objects and their associations in various CIMOMs (CIM Object Manger). Mainly this is the current Userinterface.
- OpenWBEM is used as PBNMS Server with CIMOM.
- OpenLDAP is used as LDAP Repository to store the rules of the PBNMS.

In the current installation, all of these entities are located on one server and provide an environment for testing rules (currently only the storage and loading) as well as for testing the translation modules needed for the QoS system et. al.

6.5. PBNMS in Akogrimo

In the first phase of Akogrimo we focus on the integration of the PBNMS with the QoS system to be able to provide rules using the information of the QoS system and to reconfigure the QoS system.

Phase two will then include more entities of the network infrastructure to allow more complex rules and reconfiguration based on information other than from the QoS system. Possible targets for this are the SIP infrastructure and the A4C system, the first to provide information and as a PEP (Policy Enforcement Point), the second only to provide information for the PBNMS.

7. Network Service Provisioning

7.1. Introduction

Network Service Provisioning in Akogrimo is intended to provide network functionality to Akogrimo higher layers. This means that all relevant user-network interactions (that comprises QoS, mobility, security and session management topics) must be available to the grid layers in order to enable grid-based services. Considering that QoS, Mobility and Security are covered in sections from 3 to 5, this section will address mainly session management topics, that in practise will be related to the SIP-based network support.

The concept of session has been deeply discussed within the project. Due the nature of the matters to be integrated, it is difficult to make a common and unified definition of session. It is clear that the notion of session that can be inferred from a videoconference is different from the concept of session we can extract from the process of requesting CPU cycles for performing a complex calculation.

From the network point of view, a session can be understood as the availability of exchange data between two (or more) entities. In order to enable this data exchange, there must be an agreement between these entities (i.e. for multimedia sessions, the audio or video codecs to be used) and the network itself to guarantee, for example, that the data exchange is carried out with the necessaries QoS and security. This agreement takes place during the session setup process.

As well as the conditions that were established during session setup process may change due to several circumstances (i.e. Akogrimo users can be mobile, so a user with an ongoing session may change its attachment point to the system from one access network to another, where network conditions may be completely different), there should be available mechanisms to perform a session renegotiation.

The Session Initiation Protocol (SIP) is an application-layer protocol that provides mechanisms to establish, modify and terminate sessions. In conjunction with other IEFT protocols it can provide advanced support for multimedia sessions, but it is not restricted to multimedia. These protocols are SDP, Session Description Protocol for describing multimedia sessions; RTP, Real-time Transport Protocol for transporting real time traffic and RTSP, Real Time Streaming Protocol for controlling delivery of streaming data. It can provide also user and session mobility. Next subsections are intended to describe how SIP infrastructures cooperate with the rest of the network infrastructures to provide such kind of services.

7.2. SIP session management support

One of the most important services that the network service provisioning must provide to the higher layers is session management capabilities. This implies the ability to setup, renegotiate, and terminate sessions between users.

To guarantee the quality of the communications, it is possible that some kind of network resources reservation would be needed. For example, to establish a high quality videoconference between two users, probably some access network resources must be exclusively dedicated to this communication. This implies some kind of orchestration between session management (SIP) and QoS infrastructures, which will have to interact each other. At the same time, to avoid that some users make use of services they are not authorised to use, some interface with the A4C infrastructures is envisaged. All of these interactions take place over an infrastructure that enables mobile communications with the adequate level of security.

Sessions can be initiated by the users themselves as usual; but Akogrimo requires scenarios that should provide support to enable sessions triggered from the upper layers of the architecture, the grid layers. For example, a workflow in the grid layers could decide that a communication between a doctor and a patient should be arranged. Network services provisioning must provide mechanisms to enable this kind of interactions.

This section describes this session management capabilities that the Akogrimo SIP infrastructure can provide.

7.2.1. Registration

This is a precondition for all SIP interactions. The registration process establishes the binding between the user and his/her logical location (IP address).

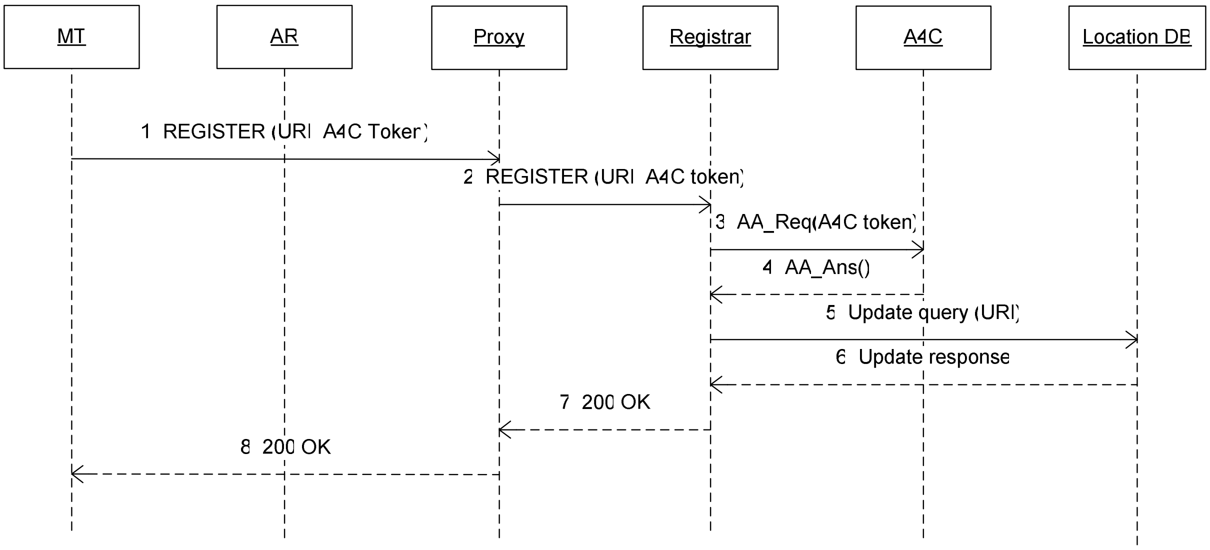

Figure 21 – SIP registration

The user wants to register itself in certain location of the domain (from a concrete device). The corresponding SIP message is forwarded to the SIP Server (through the access router and the SIP proxy), which analyses the request and determinates to inform to the embedded Registrar Server. To know if the user is authorised to use Akogrimo SIP infrastructures, a query to the A4C takes place, using the A4C token that should be included in the SIP REGISTER message. After a success authorisation, this element performs a location database updating.

7.2.2. Session Setup

Session setup is the central operation of the SIP infrastructure. When QoS is required, we can distinguish two scenarios, depending on the element that request for QoS:

- Terminal driven
- Server driven

Terminal driven scenario is depicted below. We assume that both terminals are registered. In order to simplify the diagram, and due the simplicity of the proxy behaviour, we have grouped all SIP entities (and called them SIP server).

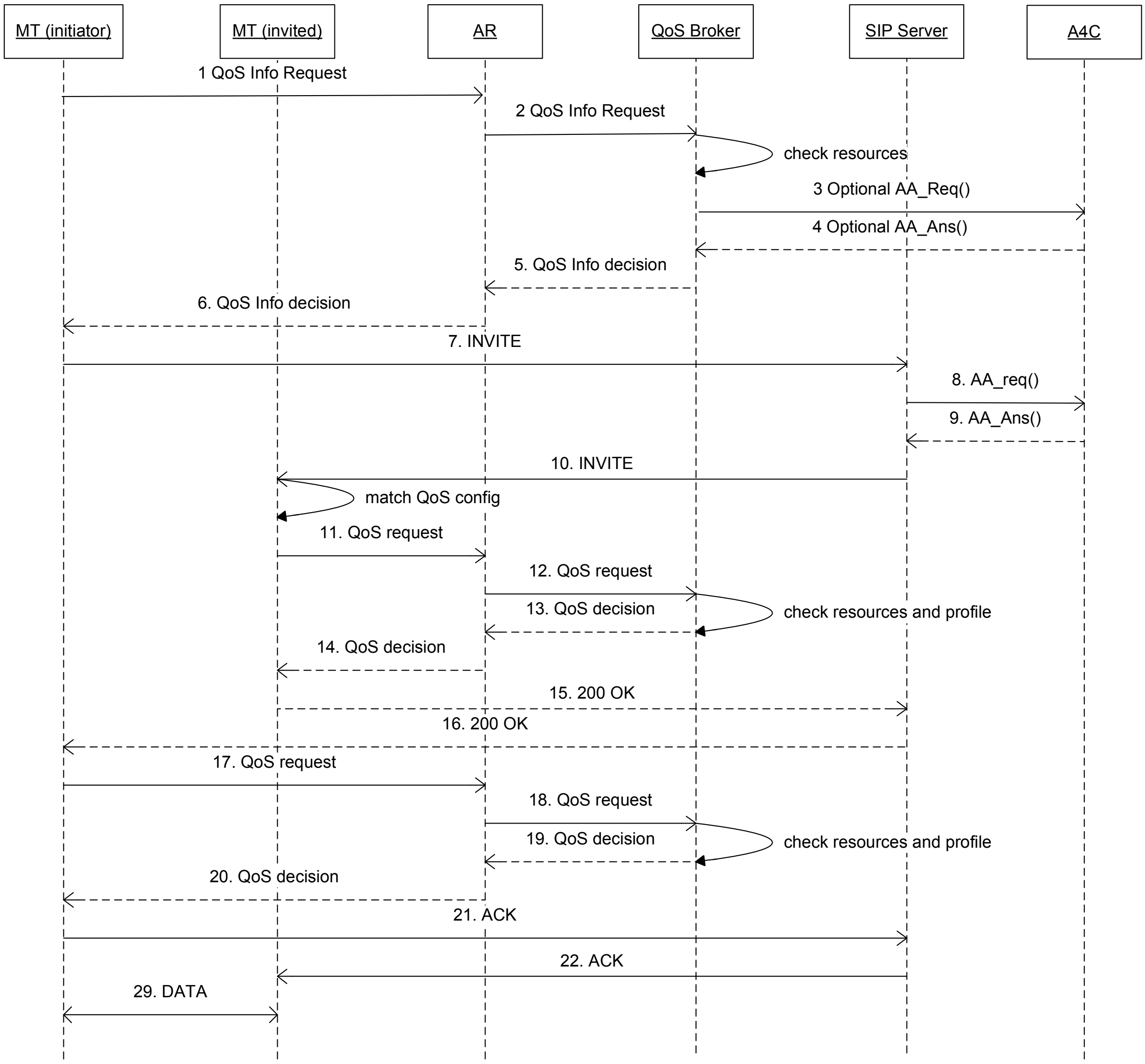

Figure 22 – SIP session setup (terminal driven)

A user that wants to start a multimedia session with another user would open his appropriate application and start the call. The user's terminal would first of all check if he is authorized by the QoS Broker; the session may be denied if network load does not allow it or if the user has exhausted his resources (bandwidth, total data used, etc.). Then, it sends a SIP request to the SIP proxy, which first of all would have to be authorized. Supposing it was indeed authorized, the SIP proxy would then forward the request to the appropriate user's terminal. After that message exchange, the SIP proxy communicates with the destination user's terminal and starts the normal SIP message exchange. When the SIP initiation process is complete, the communication is direct between the two users' terminals (AR's are involved, but only their routing functionality).

Two alternatives to check the user profile and to be authorised to use the service:

3. SIP server request for authorisation to the A4C (8, 9).
4. QoS Broker request for authorisation to the A4C when QoS is required (3, 4)

Next figure shows a simplified server driven scenario.

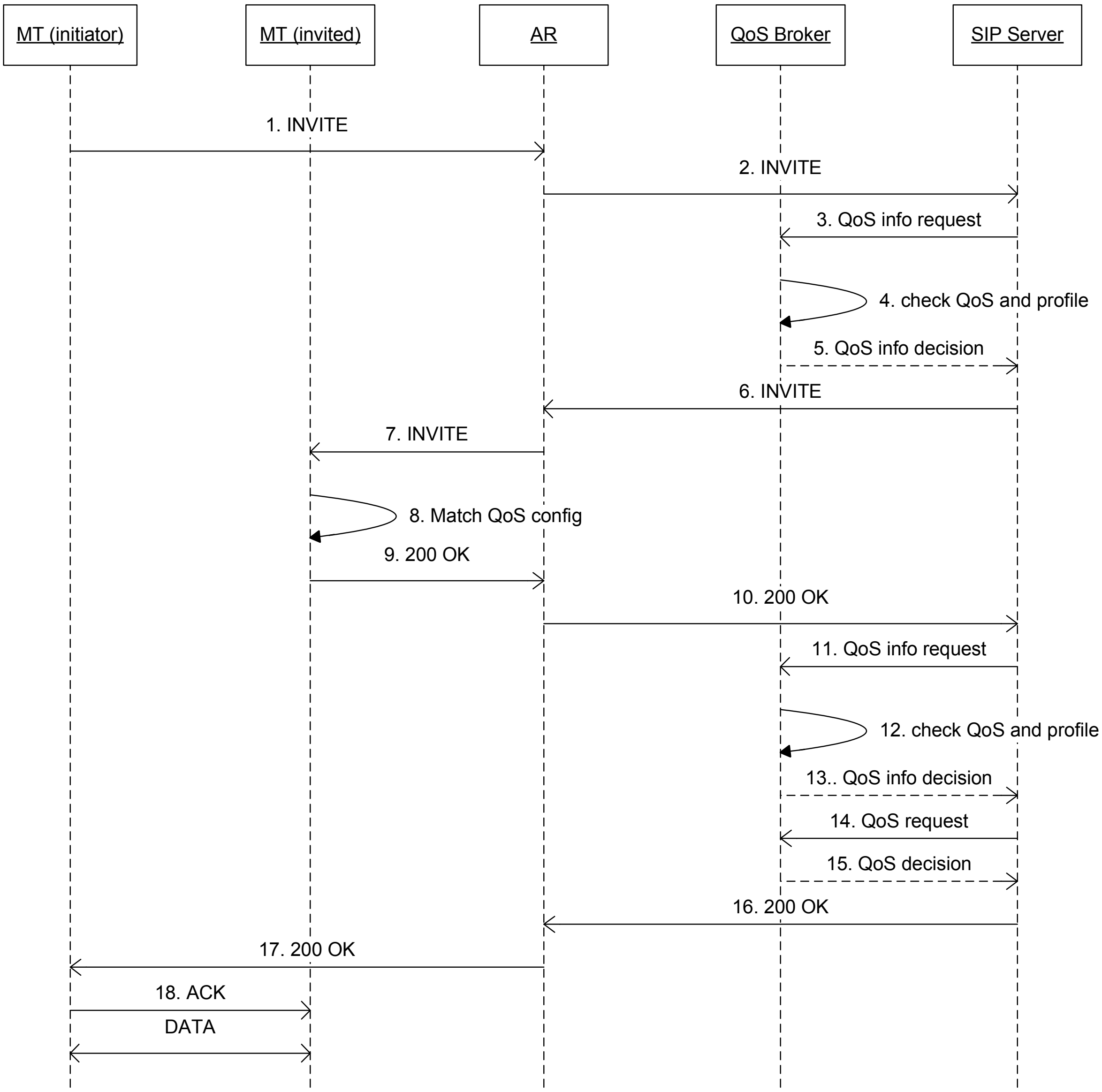

Figure 23 – SIP session setup (server driven)

In this case the initiator includes in the session initiation message the preferred QoS configuration in preference order (initial offer). When the server receives the message, it performs a QoS query info and modify the offer if needed, forwarding the initiation message to the destination (7), which considers the received offer and sends its preferences in the reply. After the reception of this message in the server (10), the preferences of both users are known, so it is possible to perform the resources reservation at this point.

In order to perform the QoS queries, the SIP server have to extract the QoS requirements from the session description protocol. For multimedia sessions, this implies the SDP body parsing of the incoming INVITE; but SIP is not restricted to multimedia, so server driven scenario supports implies to have such kind of parser per each kind of session description protocol that can be used in Akogrimo. For scalability purposes, the terminal driven scenario is preferred because the SIP application running on the terminal will be aware of the kind of session description protocol being used, so it can perform easily the mapping between session and QoS parameters.

The scenarios described here illustrate the terminal triggered scenarios. But as mentioned, the network layer should offer facilities to setup sessions not triggered by the end-users themselves.

The Workflow Manager (WP44) will invoke some "SIP aware" Web Service (WS App in the diagrams) to put in contact two SIP entities. This WS will receive a SOAP (over http) query from the Workflow Manager with the identity of the users to be put in contact and will start a SIP process to arrange the desired call.. This implies that the entity in which this application runs includes a SIP UA and a SIP application which implements the SIP-related logic.

This application will not be included as part of the SIP server for simplicity (make the SIP infrastructures as simple as possible) and to decouple SIP infrastructures from SIP applications. So we will assume that such application resides in some machine of the "grid calls" Service Provider.

Depending on the nature of the chosen SIP process to arrange the call, we will have grid initiated calls using SIP Third Party Call Control (SIP 3PCC) or using SIP REFER method. Both mechanisms are described at follows.

7.2.2.1. Grid initiated calls using SIP 3PCC

Third Party Call Control (3PCC) is described in RFC3725. Third party call control refers to the ability of one entity (the controller) to create a call in which communication is actually between other parties. Some network entity hosting the WS application described above acts as the controller after receiving a call setup query from the grid layers (not depicted in the figures) using the corresponding protocol.

RFC3725 describes different call flows depending on the nature of the parties involved in the final communication. Next figure shows the situation in which one of the entities is an automata that will answer the call immediately, like media servers, conferencing servers, and messaging servers.

Some assumptions:

- User A MT and user B MT successfully registered (which means successfully authorised to make use of Akogrimo SIP infrastructures). See section 7.2.1.
- WS App acts as the controller of the 3PCC call.
- If needed, WS App / A4C interaction during the session setup for further SIP-related authorisation. As the A4C token is needed for this, it should be done when answer from terminals is received (200 OK messages: 12-13 for user A MT authorisation and 22-23 for user B MT). This could be done also when the SIP Server receives the messages, but for simplicity and for giving the controller all the "session control" we prefer the first option.

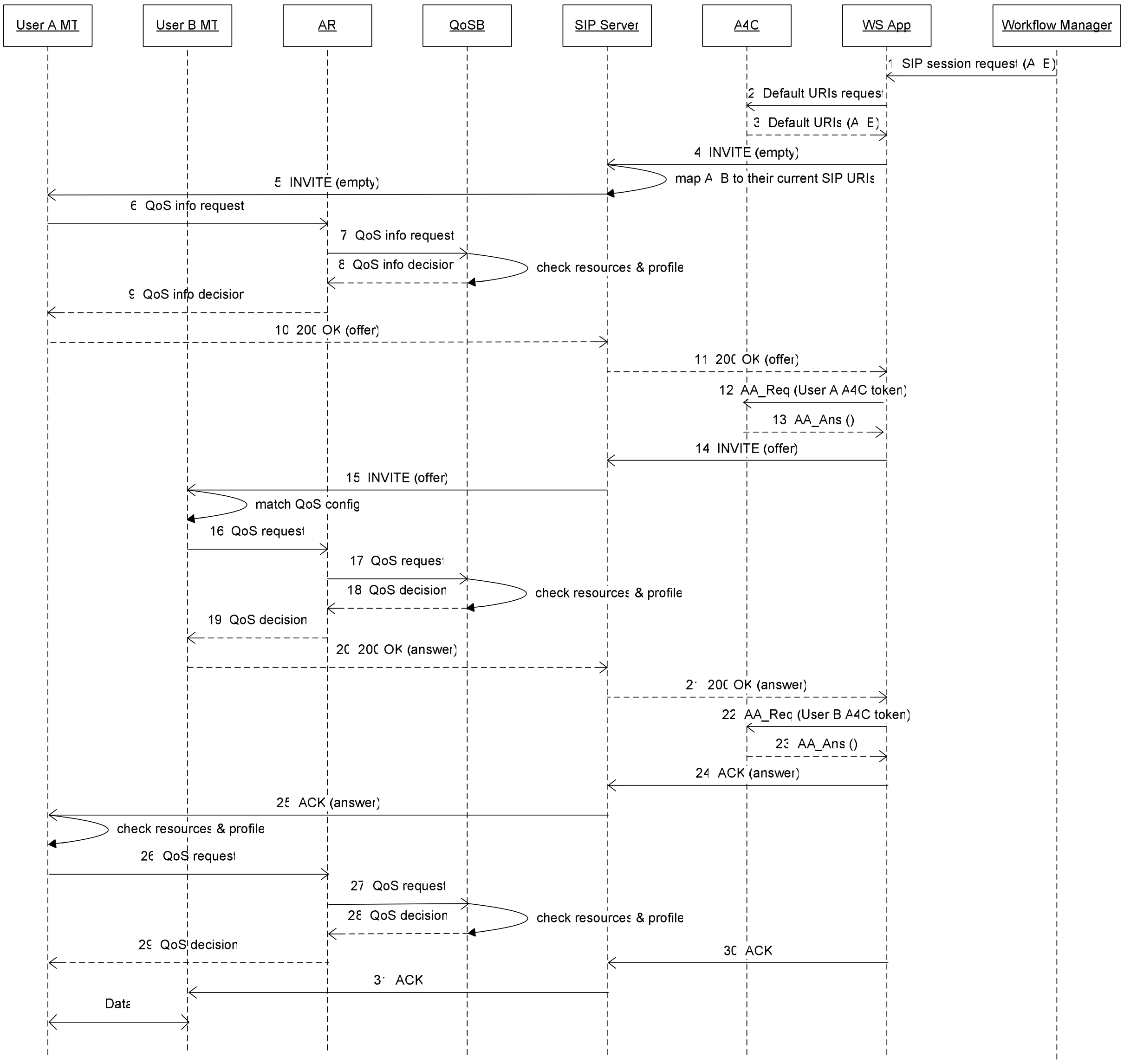

Figure 24 – Third party call control (immediate response case)

When noticed from the grid layers, and after obtaining default SIP URIs of involved users, the controller (WS App) first sends an INVITE to the first entity, user A MT (4, 5). This INVITE has no session description. User A answers with a 200 OK (10, 11) containing an initial offer, after checking for resources availability. The controller needs to send its answer in the ACK, as mandated by [1]. To obtain the answer, it sends the offer it got from user A in an INVITE to user B MT (14, 15). When user B answers, the 200 OK (20, 21) contains the answer to this offer, after the corresponding resources reservation. The controller then passes the user B answer to user A in an ACK sent to it (24, 25). Because the offer was generated by user A, and the answer generated by user B, the actual data session is between user A and user B MTs. Therefore, media flows between them.

If the user B answer is seriously delayed, user A MT can interpret that the communication has failed. This situation takes place because the controller cannot send the ACK to user A MT right away. This causes user A MT to retransmit the 200 OK responses periodically until certain timeout is reached and the call is considered to have failed. That is the reason why this is a suitable mechanism when user B is an automata.

Next data flow depicts the recommended solution when both entities are humans.

The same assumptions that described for the automata case apply here.

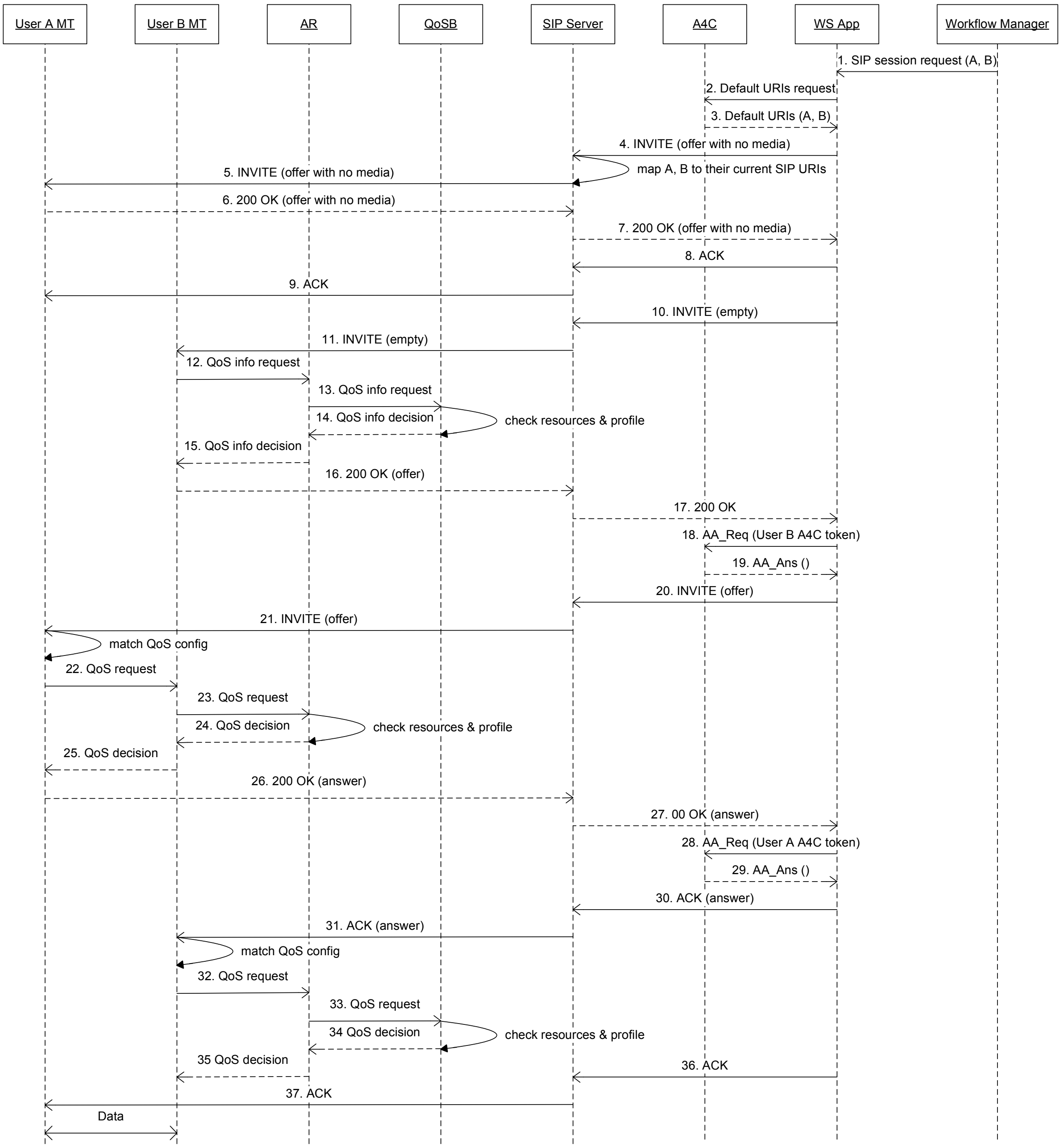

Figure 25 – Third party call control (no immediate response case)

WS App receives the query to put in contact Akogrimo users A and B (1). After requesting the default SIP URIs of the involved users (2, 3), it sends an initial INVITE (4) to one of the users through the SIP server, containing a SDP with no media at all. This is valid, and implies that the media makeup of the session will be established later through a re-INVITE (20, 21). The SIP server maps the default SIP URIs to the current SIP URIs, and redirects the INVITE (5) to the user.. Once the INVITE is received, User A MT is alerted and answers with a 200 OK (6, 7) with no media either. This is acknowledged by the controller (8, 9).

The controller then sends an empty INVITE to User B MT - without session description (10, 11). After checking for resources availability (from 12 to 15), a 200 OK is sent, containing its session offer (16, 17). This answer is used to create a re-INVITE back to user A MT (20, 21), which responses with the definitive session setup parameters (26, 27). This definitive answer is sent in an ACK to user B MT (30, 31) which is able to perform the corresponding QoS reservations (from 32 to 35). MT1 transaction is also acknowledged (36, 37).

As depicted in the message sequence chart, the element which makes the first "effective" offer is user B MT (16, 17), so there are no retransmission problems if user B does not answer immediately. In this case, the entity that effectively answers the call is user A MT(26, 27). User A has been previously alerted (4, 5), and this minimizes the probability that user B MT interprets that the session setup have no success due to a big delay in the user A answer to the reINVITE.

Once the calls are established, both participants believe they are in a single point-to-point call (MTx – Controller). However, they are exchanging media directly with each other, rather than with the controller. The controller is involved in two dialogs, yet sees no media.

Since the controller is still a central point for signalling, it now has complete control over the call. If it receives a BYE from one of the participants, it can create a new BYE and hang up with the other participant. Similarly, if it receives a re-INVITE from one of the participants, it can forward it to the other participant.

But the 3PCC approach has some inconveniences:

- Need for synchronisation: how the controller (WS App) knows it can send the second ACK (38) – which enables user A MT to send packets - to avoid sending before the final QoS configuration for user B MT is completed? Without this synchronisation, user A would be able to send packets after network resources for user B were ready, so some packets could be lost.
- WS App should control the session status (all SIP messages between A and B before and during session will go through the 3PCC controller).

7.2.2.2. Grid-initiated calls using SIP REFER

It is simpler and avoids both the synchronisation problem of the ACKs and no session control is needed.

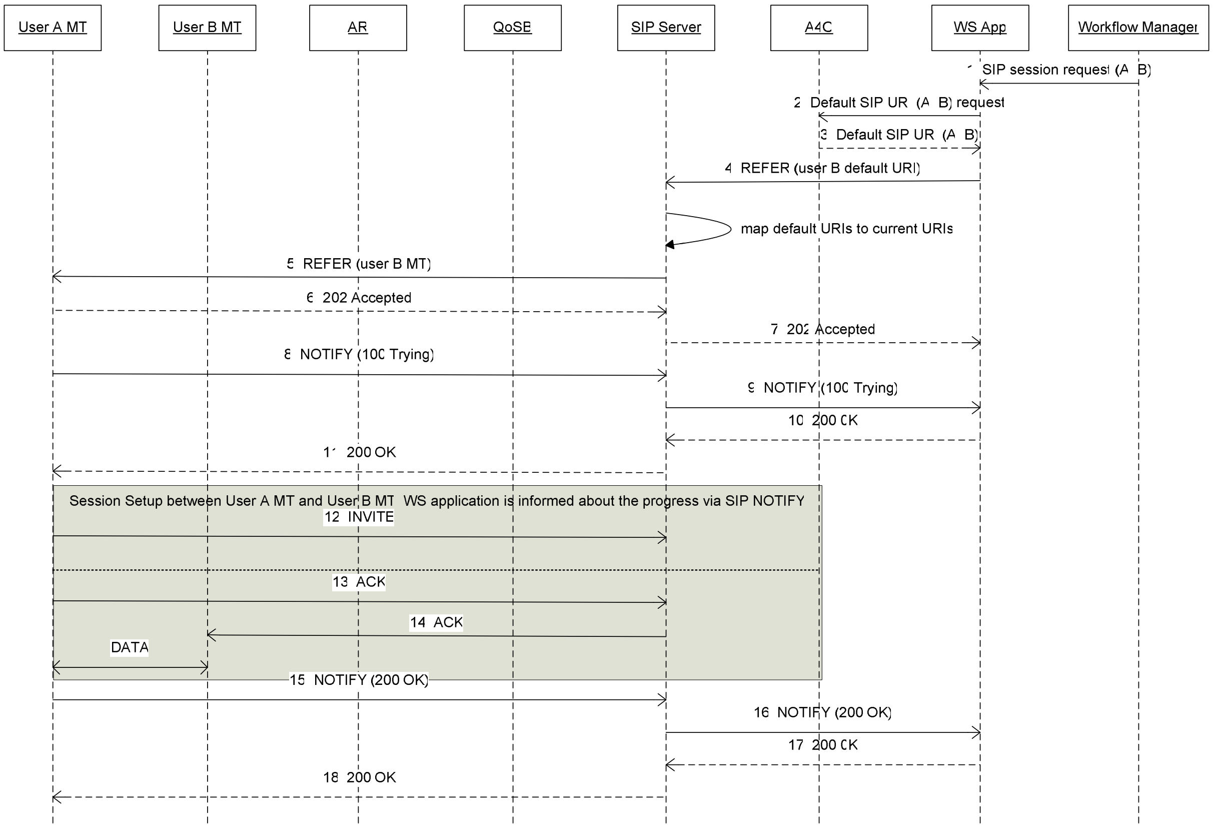

Figure 26 – Grid-initiated calls using REFER

The following assumptions are considered:

- WS App SIP User Agent and (at least) one of the user terminals involved support SIP REFER. So this is a requirement for Akogrimo SIP terminals initiating grid calls.
- User A MT and user B MT successfully registered (which means successfully authorised to make use of Akogrimo SIP infrastructures).

WS App receives the query to put in contact Akogrimo users A and B (1). After requesting the default SIP URIs of the involved users (2, 3), it sends a SIP REFER message (4) to user A through the SIP server, indicating that a session with user B should be initiated. The SIP server maps the default SIP URIs to the current SIP URIs, and redirects the REFER (5) to the user A MT (current location of user A). If the session setup is accepted on user A MT, it sends a 202 Accepted response (6, 7) and starts a standard session setup process with user B MT (from 12 to 14 in the figure, not all messages depicted). WS App is informed about the transfer progress via NOTIFY messages (8, 9, 15, 16) because REFER method creates an implicit subscription. When WS App is informed about the transfer success (16), the process finishes.

If no special requirement involving a detailed call control are imposed from the grid layers, the more simple and less conflictive REFER mechanism will be implemented, at least for the first phase of the project.

7.2.3. Session Termination

SIP session can be terminated by any of the involved entities in the communication. This can be achieved by sending a BYE message, as depicted in the figure.

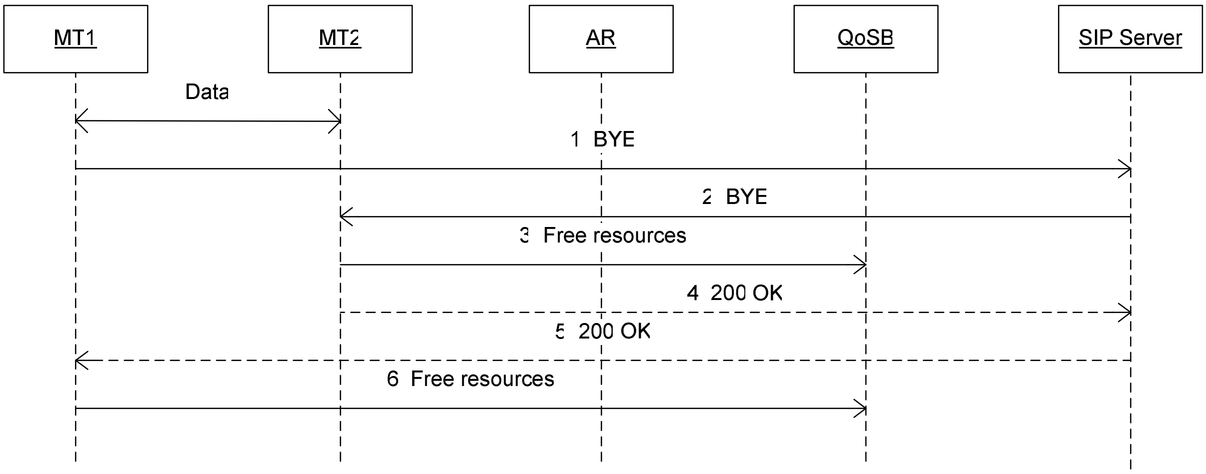

Figure 27 – Session termination

In the figure, SIP server is acting as a proxy and reserved resources are freed by the terminals. MT1 wants to terminate the existing session, so it sends a BYE message (1, 2) which is received by MT2 (3, 4), which queries to a resources de-reservation and delivers the response (6). When received at MT1 (9), it can query for resources de-reservation. This message does not need a response from the QoSB because no further actions are needed.

The call flow for the 3PCC case (if this mechanism is finally used in grid calls) is depicted below.

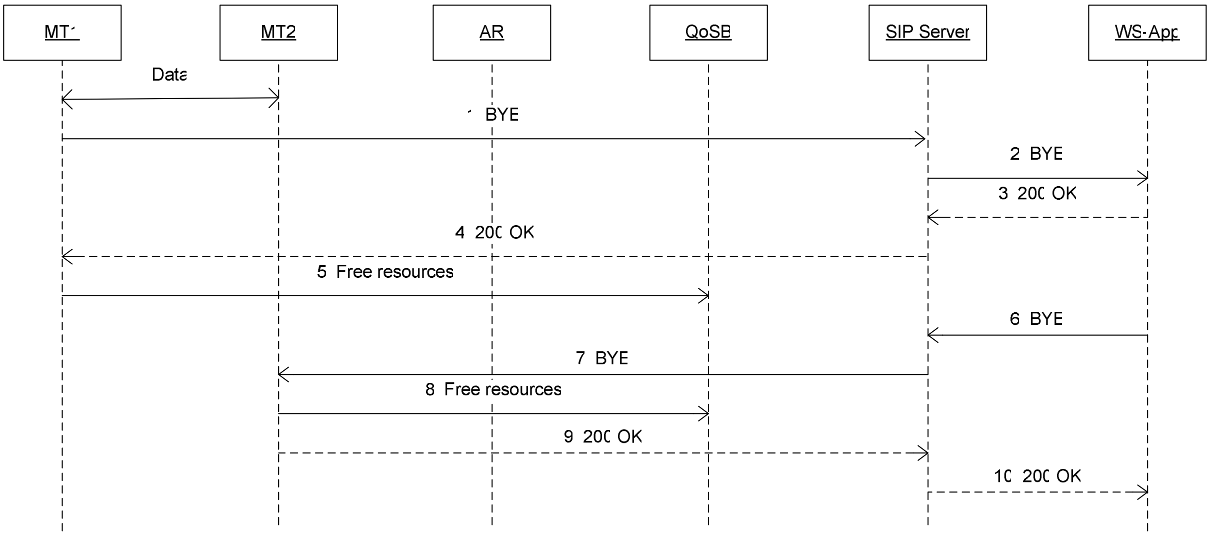

Figure 28 – Session termination (3PCC case)

In this case, the controller (WS-App) forwards the BYE message it receives from MT1 (1, 2) to MT2 (6, 7). In both cases mobile terminals behaviour regarding QoS de-reservations is the same: the free resources query is sent after receiving the response if the MT initiates the termination (3, 4) or when receiving the BYE message itself if not (6, 7).

7.3. Session Mobility

Session Mobility is the seamless transfer of media of an ongoing communication session from a source device (the element that is currently carrying a session) to a target device (the entity which will support the session after the transfer). It implies implicitly device mobility, but we will reserve the term session mobility only when ongoing sessions are present.

There are several circumstances in which a user may want move ongoing sessions from one device to another. For example, having a videoconference in his mobile terminal, a user discovers a large video monitor and decides to move the audio and video output streams to it. If the user has to abandon the place in which the large monitor is, he may want to move the session again (currently ongoing in the large monitor) to his local mobile device.

Session mobility scenarios can be classified attending to different criteria:

- Depending on which device initiates the mobility request and which device was originally supporting the communication, we can distinguish between session transfer and session retrieval. When transferred, sessions are moved from the source device (which currently supports the communication) to the target device, in response to a request from the source device itself; when retrieved, sessions are remotely transferred from a remote device (source device) to another one controlled by the user. In this case, the element which originates the mobility request is the target device, that is, the one which currently does not support the communication. Retrieval may imply to return a session to the device in which originally it was supported (as described in the example) or to another different that had not previously carried it. For example, a participant in an audio call on his IP phone may leave his office in the middle of the call and transfer the call to the mobile device as he is running out the door.
- Depending on the number of target devices, we can have full session mobility or partial session mobility. Full session mobility takes place when all session media are completely transferred to a single target device, as described in the initial example; but session media may also be split across multiple devices. For instance, a user may only wish to transfer the video of his session while maintaining the audio on his PDA. Alternatively, he may find separate video and audio devices and wish to transfer one media service to each. We refer to this situation as partial session mobility. Furthermore, even the two directions of a full-duplex session may be split across devices. For example, a PDA display may be too small for a good view of the other call participant, so the user may transfer video output to a projector and continue to use the PDA camera

Session mobility involves transfer and retrieval of an active session, as well as full or partial mobility.

Mobility is a crucial topic for the Akogrimo project. Most of the mobility support will be provided by the MIPv6 infrastructures, as defined in Section 3. But MIPv6 does not offer support for session mobility as described, so session mobility will rely on the SIP infrastructures. This means that terminal and user mobility will be available for all applications, while this feature will be available only for SIP-aware applications.

Next section describes SIP capabilities to support session mobility.

7.3.1. SIP Session Mobility support

As mentioned, using SIP it is possible to perform ongoing session transfers between different devices. The most suitable methods for supporting Session Mobility are third-party call control (usage a different SIP entity from finally involved in the data transfer) and the SIP REFER method.

When using third-party call control, the SIP external entity which controls the communication is the source terminal itself. It is also called Mobile Node Control mode. The source device arranges separate SIP sessions with the target and the remote devices, but media stream is established between both of them. This is a similar situation that described in 3PCC session setup, when an external entity (the SIP server in this case) triggers a session setup process that ends in a data exchange between two different endpoints. This approach makes use only SIP methods defined in RFC 3261 (basic SIP specification), but requires the controller to remain active to maintain the sessions and perform any further actions, like termination or renegotiations.

Sessions could be transferred also using the SIP REFER method [SIP03], which avoids the requirement of having the source device active to maintain the session. This mechanism is also known as Session Handoff mode. This is useful if a user may need to transfer a session completely because the battery on his mobile device is running out. Alternatively, the user of a static device (like a video wall) who leaves the serving area may wish to continue the communication in his mobile device, so it performs a session transfer to it. In such cases, this approach is really useful.

7.3.1.1. Mobile Node Control mode

Next figure shows the sequence diagram that corresponds to a session transfer to a single device (full session transfer). For simplicity purposes, and considering that the AR will route all SIP messages to the SIP server, direct interactions have been depicted between SIP terminals and SIP server. It is supposes also that the target device is ready to provide an immediate answer.

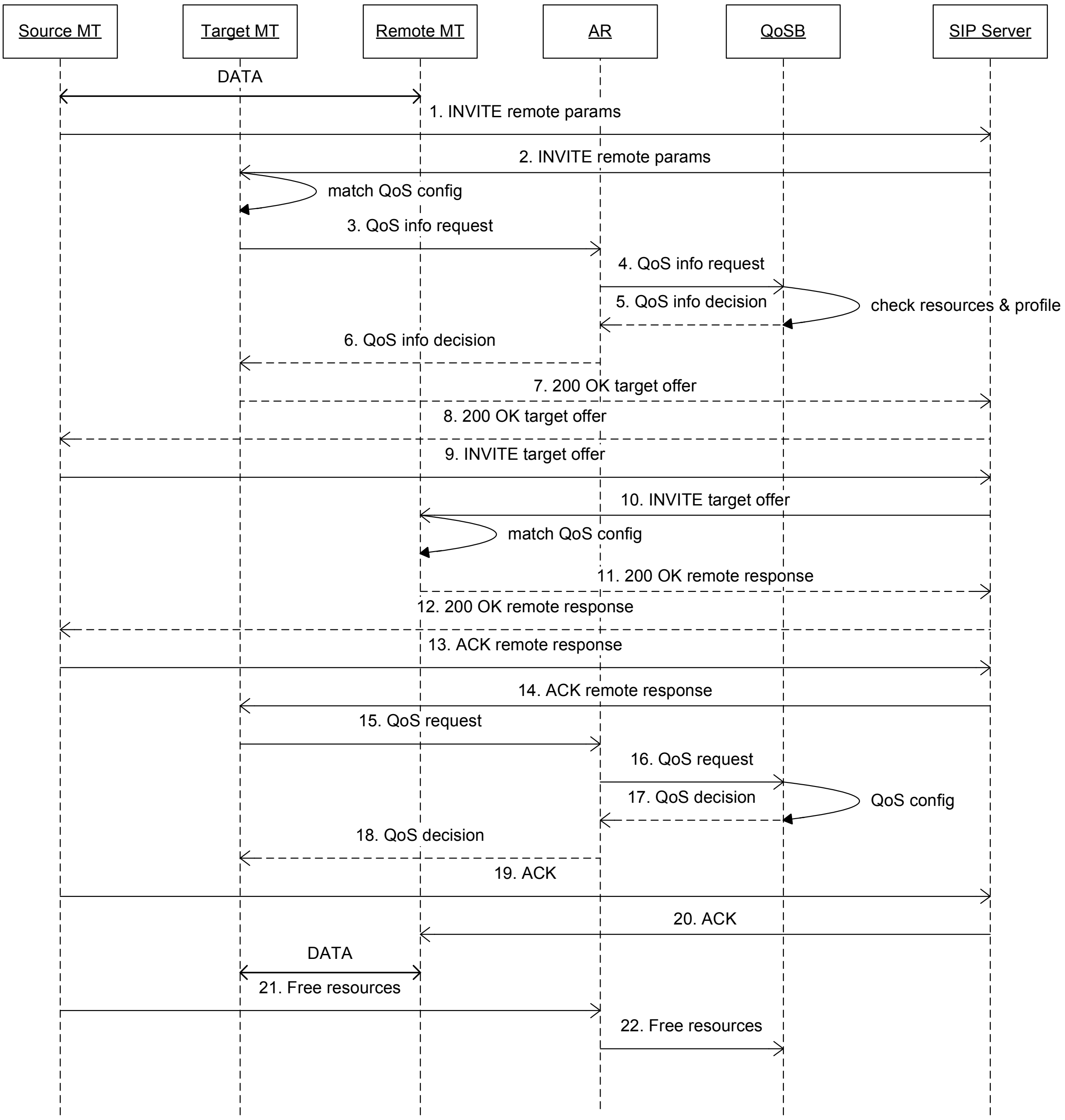

Figure 29 – Mobile Node Control mode, session transfer

Session is established between source MT and remote MT, when source MT decides to transfer this ongoing session to target MT. It sends an INVITE (1, 2) message to the target MT containing current session parameters with the remote MT, that after checking the QoS configuration and the resources availability (3, 4, 5 and 6) delivers a 200 OK response with its own offer (7, 8). The source MT routes this offer to the remote MT using a re INVITE, which contains the target device SIP URI (9, 10). If accepted (11, 12), the source MT sends an ACK to the target device (13, 14), which reserves the corresponding resources if needed). The offer was generated by target MT, and the answer generated by remote MT, so data can flow between them. After delivering the ACK to the remote terminal (19, 20), source MT can free reserved resources.

Target offer may imply some kind of QoS reconfiguration in the remote side (i. e. the codec being used is not supported by the target terminal, and the offered one implies a lower bandwidth usage). This can take place before sending the response (11).

Source MT can retrieve the session later by sending a re INVITE to the remote terminal with its own session parameters. This causes the media streams to return. Then it sends a BYE message to the target MT to free previously reserved resources.

7.3.1.2. Session Handoff mode

Next figure shows the sequence diagram that corresponds to a session transfer to a single device (full session transfer), using Session Handoff mode (SIP REFER). For simplicity purposes, and considering that the AR will route all SIP messages to the SIP server, direct interactions have been depicted between SIP terminals and SIP server.

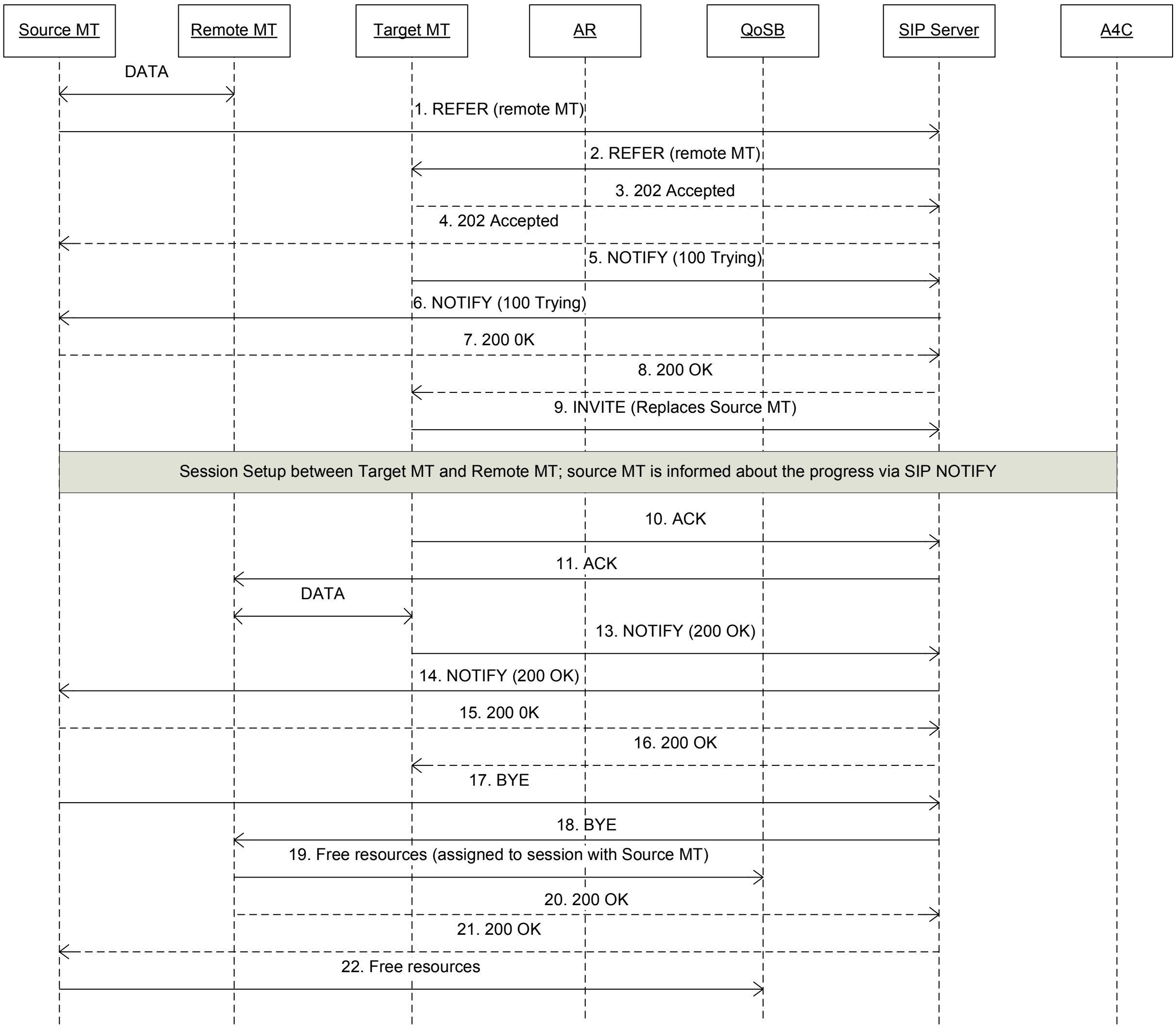

Figure 30 – Session handoff mode, session transfer

There is a session currently established between Source MT and Remote MT, and Source MT wants to move this session to Target MT. To achieve this, a REFER message is sent from Source MT to Target MT (1, 2), indicating that a session with Remote MT should be established. If the session transfer is accepted on Target MT, it sends a 202 Accepted response (3, 4) and starts a standard session setup process with Remote MT indicating that this new one replaces existing one with Source MT (9). Source MT is informed about the transfer progress via NOTIFY messages (5, 6, 13, 14) because REFER method creates an implicit subscription. When Source MT is informed about the transfer success (14), starts a standard Session Termination process with Remote MT (from 17 to 22), which frees involved resources.

7.4. Personal Mobility

Personal mobility is the user's capacity to send and receive calls and access subscribed telecommunication services, regardless of the device being used. Besides, it is the network ability to identify the user when he is moving. This ability is based on the use of a single personal identity.

The personal mobility can be defined as the capacity to locate the user, regardless of his position, as well as of the device which he is using. So, the user can reach a service, from PC, PDA or from a mobile phone, and also regardless of the access network, because terminals can access the Akogrimo network from a variety of them.

SIP plays a very important role about personal mobility, because SIP is capable to translate to a single overall address all possible physical user connection addresses. For example, the SIP URI user@192.0.2.4:5060 when accessing from the PDA which have that IP address, the SIP URI user@192.0.2.5:5060 if accessing from the user PC (with IP address 192.0.2.5),…all of them, different possible user locations, are mapped to the overall address user@homedomain. Thus, the services are not bound to an identifier of the device but to a single overall address. So a certain user can have different "SIP addresses" (SIP URIs) in different domains, or when accessing from different devices and the system will be able to reach them. This is possible because, when the physical connection address reaches the SIP Server, this translates it to the single overall address.

These translation mechanisms of the SIP servers are basically mapping mechanisms, which use personal databases that recognize different address as the same. That is, it maps the SIP URI associated to a certain device to the "default URI", single overall address, or Address of Record (AoR) of the user.

These mechanisms relays on the SIP REGISTER method. When the user performs a registration, indicates both the AoR of the user (which is provided in the "To" header field) and the SIP URI of the device being used (which is provided in the "Contact" header field). Then, the SIP Server updates the list of bindings of the received AoR with the new location.

Most usual "Contact" header field has the form "user@ip_address:port", because if a name is used instead of it (for example, user@pda-domain.com) requests will be sent to that network location, and there must be some other network entity (like a DNS) to perform the corresponding mapping between the name and the IP address.

The following figure provides an example: a user that start accessing from his PDA, and then he turns on his PC. Finally, he decided to turn off the PDA. For simplicity, network authentication process for each terminal (which provides a valid A4C token to the user terminal) is not depicted.

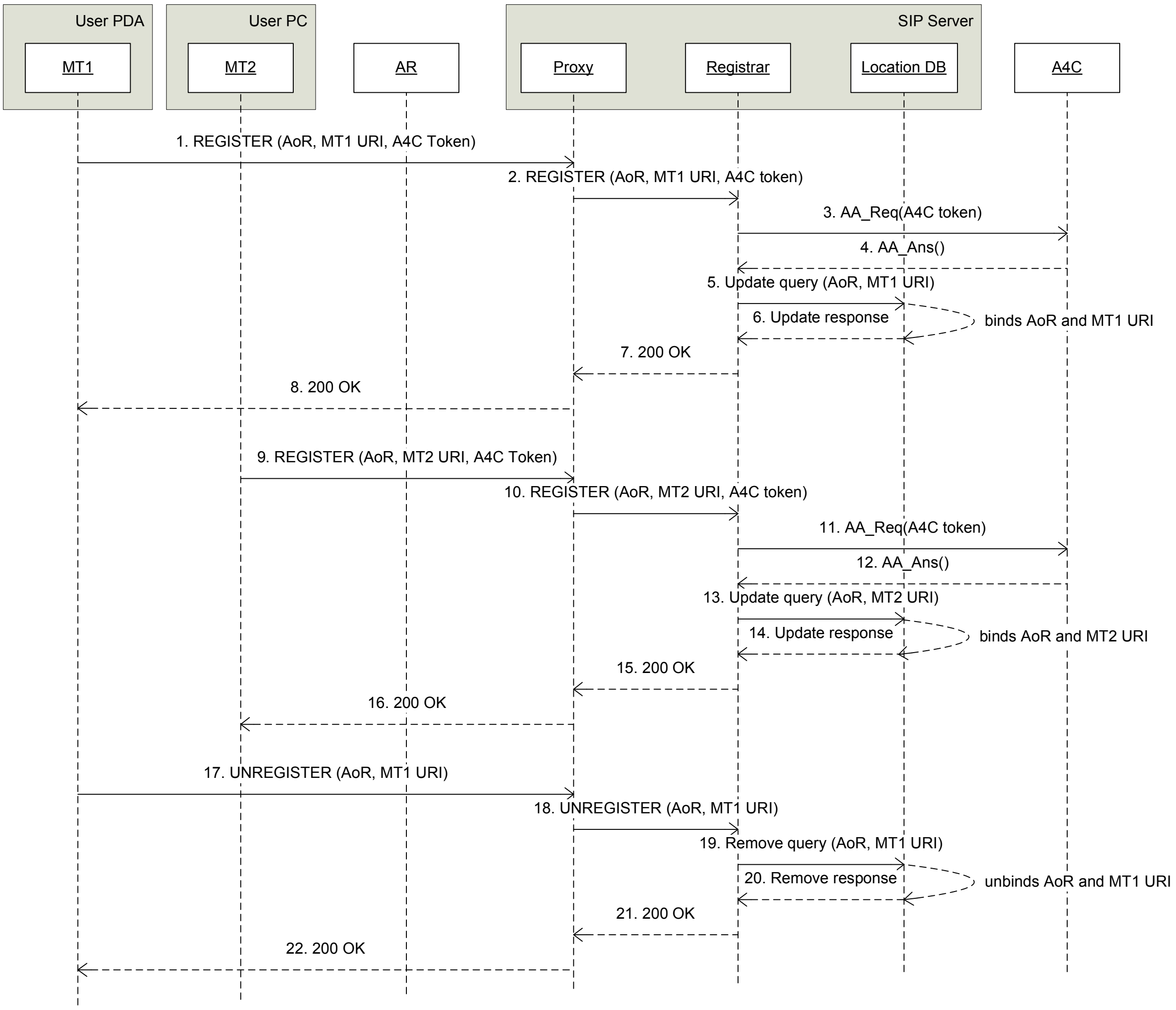

Figure 31 – Personal mobility

The user starts a standard SIP registration from its PDA, as described in 7.2.1 (messages from 1 to 8). At this point the user is accessible (for example, if someone call him) at the PDA SIP address, which was bound to the AoR of the user (5, 6). Then he decides to turn on his PC, so an identical process takes place (from 9 to 16) considering in this case the SIP URI of his computer. At this moment, the user is accessible in both terminals, so if a SIP call arrives, the SIP Server will forward it to the whole set of active locations; consequently, both terminals will ring.

Finally, he decides to turn off the PDA, so the terminal sends an unregister request (17, 18). Formally, it consists on a special REGISTER message with an indicative flag). When received, the Registrar forces the Location Database to unbind the PDA URI from the user AoR (19, 20). From now on, the user will be accessible only in his PC.

8. Multi-provider case

For the first phase of Akogrimo, different administrative domains, administered by different providers are not considered. Introduction of multiple administrative domains poses a significant amount of challenges. First of all, there must exist an agreement between the original user's domain and the visited domain. When such an agreement is in place, authentication and authorization requests are forwarded by the visited domain to the user's original domain.

Another issue is that different domains may have different QoS levels, therefore some conversions may be necessary when a user moves to a foreign domain or even when that user wants to contact with a foreign domain's user. When a QoS reservation is requested, the origin domain must contact the foreign domain to assert that the user in the foreign domain is able to attain a suitable QoS level.

In general, when a user is located outside his home domain, all signalling is more complicated and takes longer than if he were in his origin network. There are, however advantages to the multi-domain scenario. Besides the obvious advantage of a user being able to communicate when located outside its home domain, some other advantages are foreseeable. One such advantage is, for example, when a user is in an area where there are multiple networks available. In that case, the user may choose to move to another network which has a stronger signal. Another possibility is cost efficiency; in that case the user may choose to switch from e.g. an expensive UMTS network to a Wi-Fi network.

9. References

[3PCC] RFC 3725 “Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)”, J. Rosenberg, J. Peterson, H. Schulzrinne, G. Camarillo. http://www.ietf.org/rfc/rfc3725.txt?number=3725

[AAA] RFC2903 “Generic AAA architecture”, C. de Laat, G. Gross, L. Gommans, J. Vollbrecht, D. Spence, http://www.ietf.org/rfc/rfc2903.txt

[DAI] Daidalos Project, http://www.ist-daidalos.org/

[DIAM] Diameter Base Protocol, http://tools.ietf.org/wg/aaa/draft-ietf-aaa-diameter/draft-ietf-aaa-diameter-14.txt

[IKE] RFC2409, “Internet Key Exchange”, D. Harkins, D. Carrel, http://www.ietf.org/rfc/rfc2409.txt

[IPSEC] RFC 2401 “IPsec - Security Architecture for the Internet Protocol”, S. Kent, R. Atkinson, http://www.ietf.org/rfc/rfc2401.txt

[IPv6] RFC2460 “Internet Protocol version 6”, S. Deering, R. Hinden, http://www.ietf.org/rfc/rfc2460.txt

[KAME] KAME Project, http://www.kame.net

[MD] Moby Dick Project, http://www.ist-mobydick.org/

[MIPv6] RFC3775 “Mobility Support in IPv6”, D. Johnson, C. Perkins, J. Arkko, http://www.ietf.org/rfc/rfc3775.txt

[SWAN] Openswan, www.openswan.org

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

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

[SDP] RFC 2327 ”SDP: Session Description Protocol”, M. Handley, V. Jacobson, http://www.ietf.org/rfc/rfc2327.txt

[SIP01] RFC 3261 “SIP: Session Initiation Protocol”, J. Rosenberg/H. Schulzrinne/G. Camarillo/A. Johnston/J. Peterson/R. Sparks/M. Handley/E. Schooler. http://www.ietf.org/rfc/rfc3261.txt?number=3261

[SIP02] RFC 3856 ”A Presence Event Package for the Session Initiation Protocol (SIP)”, J. Rosenberg. http://www.ietf.org/rfc/rfc3856.txt?number=3856

[SIP03] RFC 3515 “The Session Initiation Protocol (SIP) Refer Method”, R. Sparks, http://www.ietf.org/rfc/rfc3515.txt?number=3515