

# **The Daidalos project and standardizing NGN in ETSI TISPAN - an overview**

Dennis Bijwaard – Lucent Technologies  
Sietse van der Gaast – Lucent Technologies

September 2005

**Disclaimer:**

The work described in this paper is based on results of IST FP6 Integrated Project DAIDALOS. DAIDALOS receives research funding from the European Community's Sixth Framework Programme. Apart from this, the European Commission has no responsibility for the content of this paper. The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

# 1 Introduction

The ETSI technical committee TISPAN (Telecommunication and Internet converged Services and Protocols for Advanced Networking) covers an area which is currently often referred to as NGN-FBI (Next Generation Networks - Fixed Broadband Interworking). Part of the work of TISPAN is to enhance the (3GPP-) IMS to become usable as a the heart for both (or combined) mobile and fixed networks, and to emulate and/or simulate and interwork with ISDN/PSTN supplementary services.

The Daidalos (Designing Advanced Interfaces for the Delivery and Administration of Location independent Optimised personal Services) project is a 6th Framework (first call) integrated project aiming to support the convergence of broadcast and mobile networks and the integration of complementary network technologies to provide pervasive and user-centered access to these services.

TISPAN aims to support the evolution from ISDN/PSTN services to the NGN networks and the integration of fixed broadband access networks with the 3GPP IMS, and therefore deals with NAT, support of IPv4, possible SIP extensions needed to support ISDN/PSTN supplementary services, Daidalos focuses more on the signaling and service aspects, while the access networks are assumed to be generic IPv6.

This paper briefly describes the goals and status of TISPAN and Daidalos, and discusses possible synergy between the solutions proposed and prototyped in the Daidalos project for the TISPAN standardization effort, especially in the area of QoS and mobility, security and AAA, broadcast/multicast and multiparty calls.

## **2 The IMS in the TISpan architecture**

### **2.1 What is ETSI TISpan?**

A Next Generation Network (NGN) is a packet-based network able to provide services including Telecommunication Services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It offers unrestricted access by users to different service providers. It supports generalized mobility, which will allow consistent and ubiquitous provision of services to users.

### **2.2 Services in TISpan**

TISpan NGN Release 1 supports the following major service capabilities:

- Session establishment and control for session based services, e.g. Real-time conversational services (voice, multi-media, messaging, etc.);
- Presence (similar to 3GPP presence services [6])
- Content delivery (e.g. Video-on-demand, video streaming, TV channel distribution);
- PSTN/ISDN migration (including replacement). This includes the simulation of a number of basic PSTN/ISDN supplementary services:
  - Originating Identification Presentation and Restriction (OIP/OIR),
  - Terminating Identification Presentation and Restriction (TIP/TIR),
  - Malicious communication Identification (MCID),
  - Anonymous Communication Rejection (ACR).

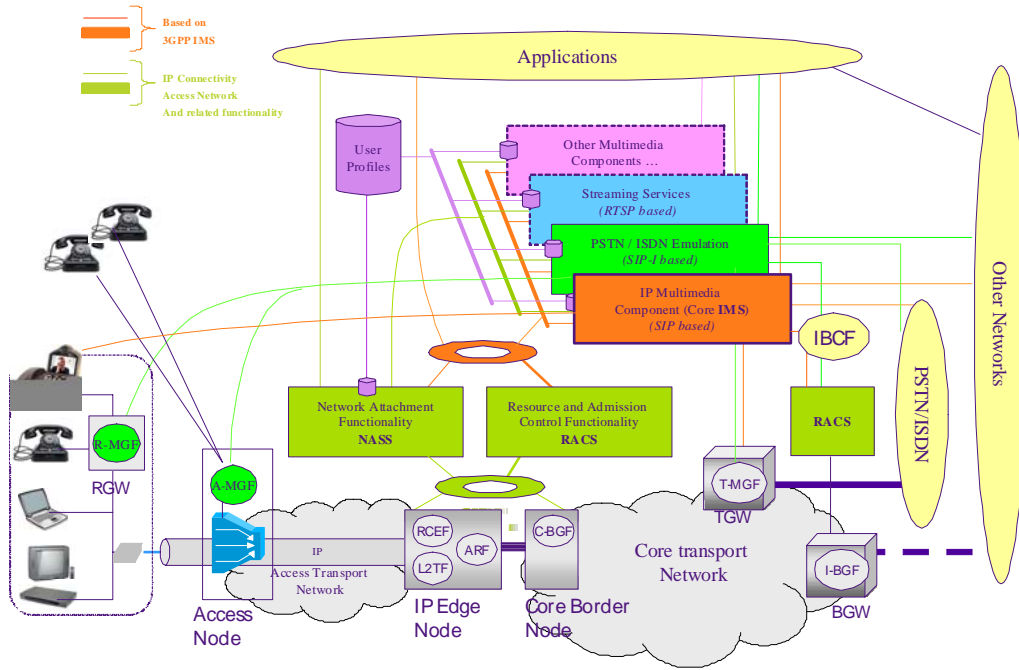
Strictly recommended services in TISpan are: like Communication Diversion, Communication Waiting, Communication Hold, Communication Barring, Completion of communications to Busy Subscriber, Follow Me and Message Waiting Indication and optional services are Conference, Advice of Charge, Closed User Group, Direct Dialling In and Trunk Hunting.

- Public Internet type services and applications.
- Conversational text (as defined by EG 202 320 (DEG/HF-00057))

NGN services are based on the 3GPP IMS (Release 6) supported services (for SIP-controlled services including presence). The existing PSTN/ISDN services are supported for legacy terminals by PSTN/ISDN emulation. NGN additionally supports content delivery and Public Internet type services.

### **2.3 The TISpan architecture**

The TISpan Network Architecture is based on the re-use of the 3GPP IP Multimedia Subsystem (IMS) Release 6 for SIP-controlled services including the control and delivery of real-time conversational services (SIP-based control). For non-SIP controlled services the NGN architecture may include additional subsystems.



**Figure 1: Overall TISPAN Architecture**

TISPAN uses a sub-system oriented approach, enabling the addition of new subsystems, to cover new demands and service classes. This also enables the import (and adaptation to) subsystems from other standardisation bodies, and provides flexibility to adjust a subsystem architecture with no or limited impact on other subsystems.

IP connectivity is provided using two subsystems:

- **The Network Attachment SubSystem (NASS) [1]**, which dynamically provides IP addresses and other terminal configuration parameters, performs IP layer Authentication and Authorisation of network access and, based on user profiles, access network configuration and IP layer location management.
- **The Resource and Admission Control Subsystem (RACS) [5]** provides admission control and gate control functionalities (including Network Address and Protocol Translation and DSCP marking). Admission control involves checking authorisation based on user profiles held in the NASS, on operator specific policy rules and on resource availability.

Service-oriented subsystems include

**The 3GPP IMS [2]**, suitably adapted to the fixed broadband access context. The resulting IMS supports the provision of SIP-based multimedia services to TISPAN NGN terminals and the provision of PSTN/ISDN simulation services. The IMS architecture is already largely access independent, but mobile network specific behaviour still exists. TISPAN works together with 3GPP using liaison statements and Change Requests to ensure that remaining (mobile) access network specific references are removed from the IMS specification and when necessary the TISPAN IMS adds functionality to ensure the interworking with both fixed and mobile access networks.

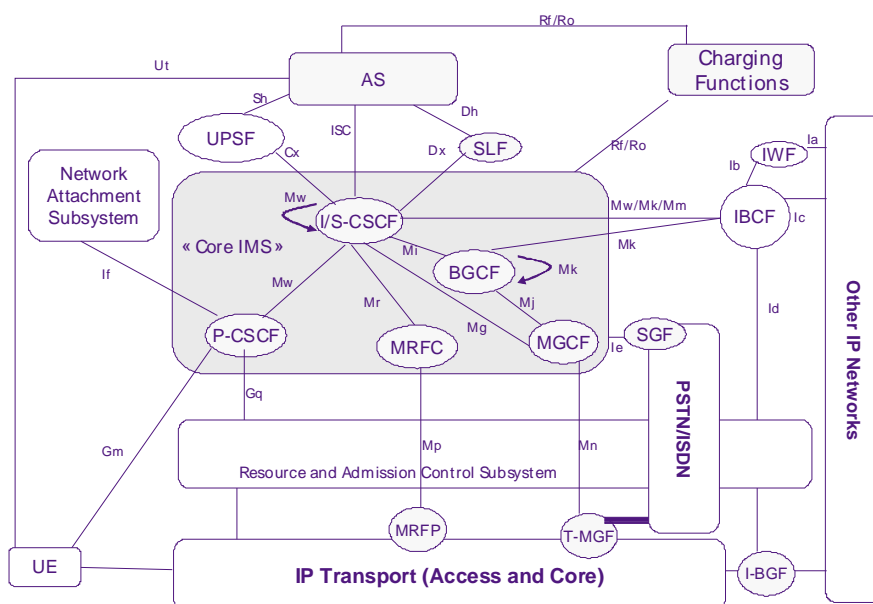
- **a PSTN/ISDN Emulation Subsystem (PES) [3]** supports the emulation of PSTN/ISDN services for legacy terminals connected to the TISPAN NGN, through residential gateways or access gateways.

- Future service-oriented subsystems may include a streaming subsystem and a TV Broadcasting subsystem.

## 2.4 Extensions to the 3GPP IMS in TISPAN

The 3GPP IMS is extended in the TISPAN NGN architecture to support additional access network types, such as XDSL and WLAN. The 3GPP IMS extensions take account of:

- The control of access networks (QoS, admission control, authentication, etc.);
- The co-ordination of multiple control sub-systems to a single core transport for resource control;
- The interworking and interoperability with legacy networks;
- Mutual de-coupling of the application layer from the session/call control layer and the transport layer;
- Access technology independence of session/call control layer and application layer.



**Figure 2: The 3GPP IMS in the TISPAN NGN architecture**

An extra network element that is introduced in TISPAN is the IBCF, the Interconnection Border Control Function. This function controls the boundary between two operators' domains. This includes interaction with transport resources (including NATP and firewall functions), through the RACS, insertion of an Interworking Function (IWF) for interworking between NGN SIP profiles and other SIP profiles or IP-based protocols like H.323, in the signalling route when appropriate, and screening of signalling information based on source/destination.

3GPP IMS elements that are impacted by the TISPAN approach are the P-CSCF and the S-CSCF. To be able to fully support PSTN/ISDN supplementary services a number of requirements and proposals for necessary SIP extensions have been brought to both 3GPP and the IETF. Other issues that have been addressed are the augmenting of P-CSCF procedures with ALG-like capabilities for supporting interactions with NATP-(PT) and the support of insertion of location information in SIP messages by the P-CSCF.

A number of issues regarding the support of Emergency Services is under investigation. These issues include the provision of a the network asserted location of a caller, prioritization or preferential treatment of emergency calls and the use of authentication of identifiers.

### 3 The IMS in the Daidalos architecture

The integrated EU project Daidalos aims to provide an environment in which mobile users can access a diverse range of personalized services transparently on top of an heterogeneous network composed of diverse network technologies. Furthermore this environment is open for service operators means to provide services.

The architecture defines a Service Provisioning Platform comprised of services for Quality of Service, Network Management, Network Monitoring, Security, Authentication, Authorization, Accounting, Audit, Charging and Multimedia. This Service Provisioning Platform makes the tools available for creating services and applications on top of integrated heterogeneous access networks. The architecture also defines functionalities and interactions necessary in and between the access networks, the Service Provisioning Platform, and the end-user terminal to make this possible. The architecture is open, modular and extensible in the sense that it is open for future refinement, incorporating optimized mechanisms and processes.

The architecture divides the overall next-generation network in administrative domains, each hosting a Service Provisioning Platform. Components in different administrative domains can co-operate when there is a service level agreement and a trust relationship between them. This cooperation is necessary to support the different services of the Service Provisioning Platform across administrative domains, including the support for seamless mobility of users, end-user terminals and multimedia sessions between administrative domains.

#### 3.1 Daidalos Architecture

This section describes the overall architecture of Daidalos. Different layers in the overall architecture have a different role, see Figure 3.

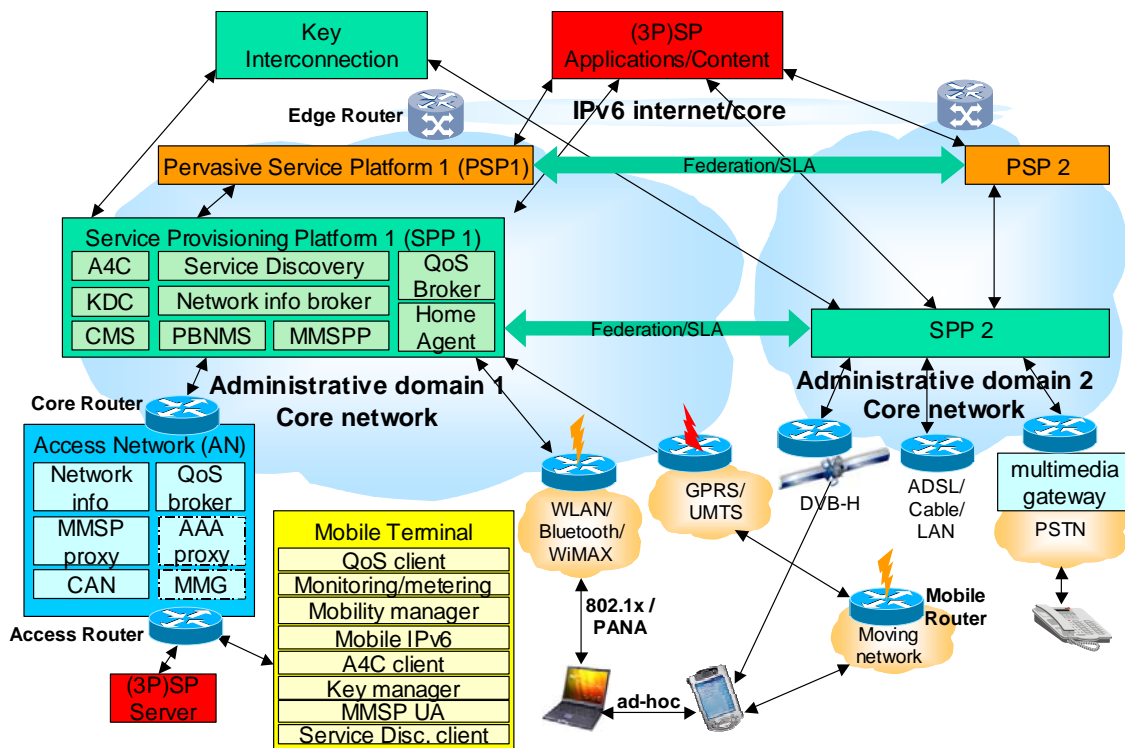


Figure 3 Overall Daidalos Architecture

Access networks covering a wide range of access technologies are connected to new service provisioning and transport platforms. In those beyond-3G mobile communication systems, Service Provisioning Platforms (SPP), Pervasive Service Platforms, Access Networks (AN), Terminals, (Third Party) Service Providers ((3P)SPs) and a Key Interconnection have to be modeled as independent entities, which operate in various organizational constellations, each reflecting different levels of content and service aggregation.

A telecom operator can take more than one role in this architecture, i.e. it could manage an administrative domain containing a number of Access Networks, a Service Provisioning Platform, and a Pervasive Service Platform and provide content and applications as a Service Provider.

### **Pervasive Service Platform**

The Pervasive Service Platform is the Service Platform for Pervasive Applications that contains functional entities to allow personalization and context-awareness.

### **(Third Party) Service Providers**

The (Third-Party) Service Providers provide applications (e.g. IMS application server) and content to the end-users, either in the domain of the telecom operator or outside (Third-Party). They can use facilities in the Pervasive Service Platform and Service Provisioning Platform to enable Single-Sign-On, to arrange QoS for provided multimedia content, to charge the user on his operator bill, to manipulate multimedia sessions and to use network information like physical user location in their applications.

The functional (Third Party) Service Provider located at the top of Figure 3, has its physical representation (Third Party) Server connected to an Access Network (AN) in the bottom, such a dedicated AN is also called Application Garden Network (AGN).

### **Key Interconnection**

The Key Interconnection enables communication between various Key Management types in different administrative domains (e.g. when cross-certification is not possible) ; for establishing a secure context between entities in different domains. For that purpose, the Key Interconnection entity provides secure inter-domain key transport. Daidalos architecture supports both asymmetric and symmetric keys (which obviously do not rely on the same keying architecture).

### **Service Provisioning Platform**

The Service Provisioning platform (SPP) is the main part of the Daidalos architecture. In this part all the service provisioning related functional building blocks are available. The Service Provisioning Platform functions as the home environment for the user w.r.t. identity, multimedia services, mobility, security, authentication, authorization, auditing, accounting and charging. The SPP contains the following components:

- Authentication, Authorization, Accounting, Auditing and Charging (A4C)
- Key Distribution Centre (KDC), this functions as PKI Certification Authority for the administrative domain
- Central Monitoring System (CMS)
- Service Discovery Server (SDS) , used to announce and discover CAN and other network services
- Network Info Broker, will in the future provide heterogeneous network context to PSP
- Policy Based Network Management Server (PBNMS)

- Multimedia Service Provisioning Platform (MMSP). This is an enhanced SIP server (or S-CSCF).
- QoS Broker
- Home Agent

### **Access Network**

The Access Network is a network comprised of the following elements:

- Access Router(s) (AR) that connect Mobile Terminals to the AN via different Access Technologies
- Control entities QoS Broker, Multimedia Service Provisioning (MMSP) proxy (i.e. enhanced SIP proxy or P-CSCF), Content Adaptation Node (CAN) , and optional AAA proxy and Network Info (a future component in the Access Network that fetches network info like UserLocation from network components in the Access Network).
- To better separate Access Network (AN) and Core Network (CN), especially when AN and CN are operated by different parties, a CoreRouter at the edge of AN as well as on the edge of CN may be required.

One or more access technologies can be available in each Access Network. A number of functional blocks are required in the Access Network to enable mobility, QoS, content adaptation, and security; i.e. network-level authentication, authorization, auditing, accounting and charging. A special type of AN is the Application Garden Network (AGN), which is used to connect servers from (3<sup>rd</sup> party) Service Provider, and would only have to contain AN components needed for the applications. The AGN on his turn can be connected to a simplified SPP instead of the full-blown one that a regular operator would have.

### **Routers**

The Access Router (AR) connects access technology to the Access Network, the Core Router (CR) connects an Access Network to the Core Network, and the Edge Router (ER) connects administrative domains to each other and/or to the internet.

### **Mobile Terminal**

The mobile terminal can connect to multiple Access Networks and make use of services in the Access Network, the Service Provision Platform, the Pervasive Service Platform and at (Third-Party) Service Providers. The mobile terminal contains functional blocks to authenticate to the network and services, to manage mobility, to initiate, maintain and adapt multimedia sessions, to reserve QoS for legacy and non-legacy applications, and for monitoring/metering.

## **3.2 QoS for Multimedia sessions**

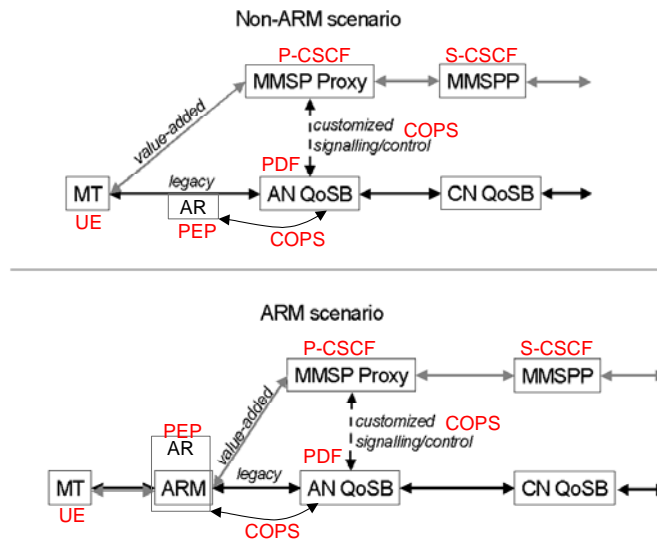
**Daidalos defines and demonstrates an end-to-end QoS infrastructure for multimedia and legacy services, with a real-time monitoring sub-system for better accuracy in the resource provisioning and management.**

The interactions between components responsible for multimedia service provisioning and components responsible for network-resource management (QoS) affect multiple layers and levels within a QoS-aware system-architecture. Different features and facets of the system have to be considered, like the way the user perceives multimedia and interacts with the application to configure it, according to his/her personal understanding for quality; the possibility of the application to map these user requirements to system parameters for presentation means (e.g. audio/video display capabilities, processing power, etc.) and for

transport purposes (e.g. serialization mechanisms for multimedia data, reservation and data-redundancy transport features, etc.); the artificial system constraints (e.g. usage policies) introduced by the network and content providers to prioritise users with different willingness to pay for services, etc.

Legacy services, which have well known and invariable set of parameters, and value-added multimedia services, which exhibit variable configuration possibilities, apply different interaction schemes with the Multimedia Service Provisioning (MMSP) and QoS. While legacy services interact only with the QoS components of the framework, the provisioning of value-added services includes higher-level service negotiations and controls within the MMSP components. MMSP components have in turn to communicate correspondingly with the QoS components to deliver specific controls for the value-added services.

Considering the signalling between the end-terminal (mobile terminal – MT) and the Daidalos framework, different scenarios are possible. These scenarios can be grouped according to the fact of the MT being assisted (advanced router mechanism – ARM) or not assisted for its signalling by the framework (see Figure 4).



**Figure 4 - MT, MMSP and QoS abstraction of the signalling paths**

The MMSP-to-QoS interface can be both integrated (in case of MT) in a single hardware entity and split (in AN) between multiple hardware components. Furthermore, the MMSP-to-QoS interface can be shared between components belonging to different programming frameworks (Java or C++). As MMSP Proxy and ANQoSBr are components, which belong to the fix infrastructure of the Daidalos framework and they themselves are not affected by mobility, the usage of such advanced communication middleware should not be critical.

The major features of the MMSP-to-QoS interface are:

- The MMSP will be able to request for resource availability and to trigger the resource reservation process in order to achieve a specific QoS level for a specific service;
- Requesting of QoS levels and new reservations will be considered as QoS re-negotiation, in some situations mobility implies QoS re-negotiation;
- The corresponding QoS entity in the terminal/network must be able to enforce a determinate QoS level, when less beneficial terminal/network conditions occur;

- The MMSP and the corresponding QoS entity should be able to free allocated resources, whenever new resources allocation is required (e.g. due to the admission of a higher priority service);
- Current QoS level status must be available to MMSP for monitoring purposes.

### 3.3 Security and AAA support

**The objective of security in Daidalos is to support value added services over heterogeneous mobile networks in a trustable and secure manner. The objective of AAA in Daidalos is to provide a future generation multi-operator, multi-network, and multi-service provider environment.**

<< summarise some more >>

Daidalos instantiates and enhances the generic AAA architecture proposed by Internet Engineering and Research Task Forces (IETF, IRTF) with single sign-on feature, and auditing and charging functionality. All components of the enhanced architecture provide for A4C services to be used in a QoS-enabled Mobile IPv6 (MIPv6) environment.

#### 3.3.i A4C Components and functionality

Four main A4C components are defined: A4C Client, A4C Server, Accounting Gateway and A4C Agent.

- The **A4C Client** resides in the Mobile Terminal and has the task to register the user to the home administrative domain. It is also responsible for signing the statements on service consumption.
- The **A4C Server** maintains user profiles including SLA, decides on registration and authorization, performs accounting and charging, and monitors SLA compliances.
- **A4C Agents** are needed to mediate between mobile A4C Clients and A4C Servers.
- The **Accounting Gateway** takes care about prepaid time- and event-based charging, and will in the future also support flow-based charging.

#### 3.3.ii Secured authentication and authorisation

In order to support the use of asymmetric cryptography for authentication, authorization, and non-repudiation of service consumption, the A4C services must interact with PKIs (Public Key Infrastructure). The protocols to be used for user authentication are EAP (Extensible Authentication Protocol) over PANA (Protocols for carrying Authentication for Network Access) between the A4C Client and the A4C Agent, and EAP over DIAMETER between the A4C Agent and the A4C Server.

#### 3.3.iii Standardized exchange of authentication information

To enable a standardized exchange of authentication information between different administrative domains and to allow for a single sign-on the use of SAML (Security Assertions Markup Language) is proposed, where the SAML Authority acts as a Trusted Third Party. After user registration, service accesses need to be authorized. Authorization of a service request must take into account the creditworthiness of the user in case the service is access through prepaid billing option. Authorization also depends on the current network conditions and this requires interaction with service

provisioning entities, e.g., QoS Brokers for network access, MMSPP for multi media services. Resource and service consumption are metered to allow for various pricing schemes. Major and required metrics are defined in the SLA. Mediation and accounting components aggregate the metered data for the purpose of charging and SLA compliance auditing.

### **3.3.iv Security Infrastructure**

In order to support the security between the network elements like routers, servers, etc., IPsec will be deployed as the basic security protocol, hence a means to distribute and manage cryptographic material not only within a single domain but also for the purpose of inter-domain interaction.

## **3.4 Broadcast/Multicast support**

**The objective of broadcast/multicast support in Daidalos is to integrate broadcast and multicast in heterogeneous QoS-enabled networks and support prepaid charging for content via broadcast/multicast.**

In Daidalos, broadcast technologies (DVB-H and MBMS) can be used as leaves of a multicast tree spanning multiple administrative domains. Daidalos supports any source multicast as well as multicasting a unicast stream from a content provider.

QoS must be reserved between all routers in the multicast tree. QoS related requirements/assumptions are:

- Support for any source and multicasting of unicast streams
- Uni-directional downlink for DVB-H and MBMS
- Source driven QoS requests
- Joining via IGMP/MLD or via content provider
- Service can be offered at different qualities, user chooses quality depending on price, codecs, etc.
- Support for Access Network specific content adaptation
- Mobility Support for source and end-points

To secure the multicast traffic through an IP network and to enable charging, a group keying mechanism is introduced. The group key will change once someone joins/leaves and periodically. Security/charging related requirements are:

- Source authentication is optional. Sensitive data (e.g. car system updates) can be integrity-protected at the application level.
- Multicast traffic encryption is required for (prepaid) charging.
- Sender access control is optional. As long as the source is “known” to the Multicast Server (formerly called play-out-centre).
- Receiver access control is required for (prepaid) charging.

Multicast routing security is obtained through the use of PKI.

## 4 Comparison

There are a number of general differences between TISPAN and Daidalos: Daidalos does not support IPv4 and also does not take into account simulation, emulation and interworking with legacy ISDN/PSTN services.

However both use an IMS like approach, as can be seen in Figure 5 and Figure 6.

In the next section a brief comparison between the approach of TISPAN and Daidalos is given for the areas of QoS and mobility, security and AAA, broadcast/multicast and multiparty calls.

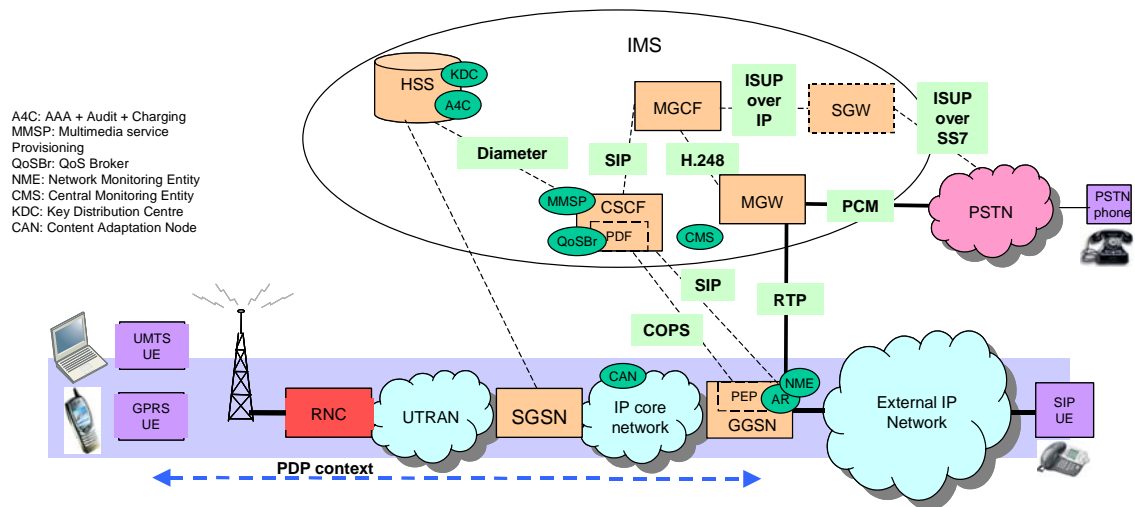


Figure 1. The 3GPP release 5 architecture.

COPS—Common open policy server  
 CSCF—Call session control function  
 GGSN—Gateway GPRS support node  
 GPRS—General Packet Radio Service  
 HSS—Home subscriber system  
 IMS—IP Multimedia Subsystem  
 IP—Internet Protocol

ISDN—Integrated services digital network  
 ISUP—ISDN user part  
 MGCF—Media gateway control function  
 MGW—Media gateway  
 PCM—Pulse coded modulation  
 PDF—Policy decision function  
 PDP—Packet Data Protocol  
 PEP—Policy enforcement point  
 PSTN—Public switched telephone network

RNC—Radio network controller  
 RTP—Real-Time Transport Protocol  
 SGSN—Serving GPRS support node  
 SGW—Signaling gateway  
 SIP—Session Initiation Protocol  
 SS7—Signaling System 7  
 UE—user equipment  
 UMTS—Universal Mobile Telecommunications System  
 UTRAN—UMTS Terrestrial Radio Access Network

Figure 5 –3GPP architecture with Daidalos terms

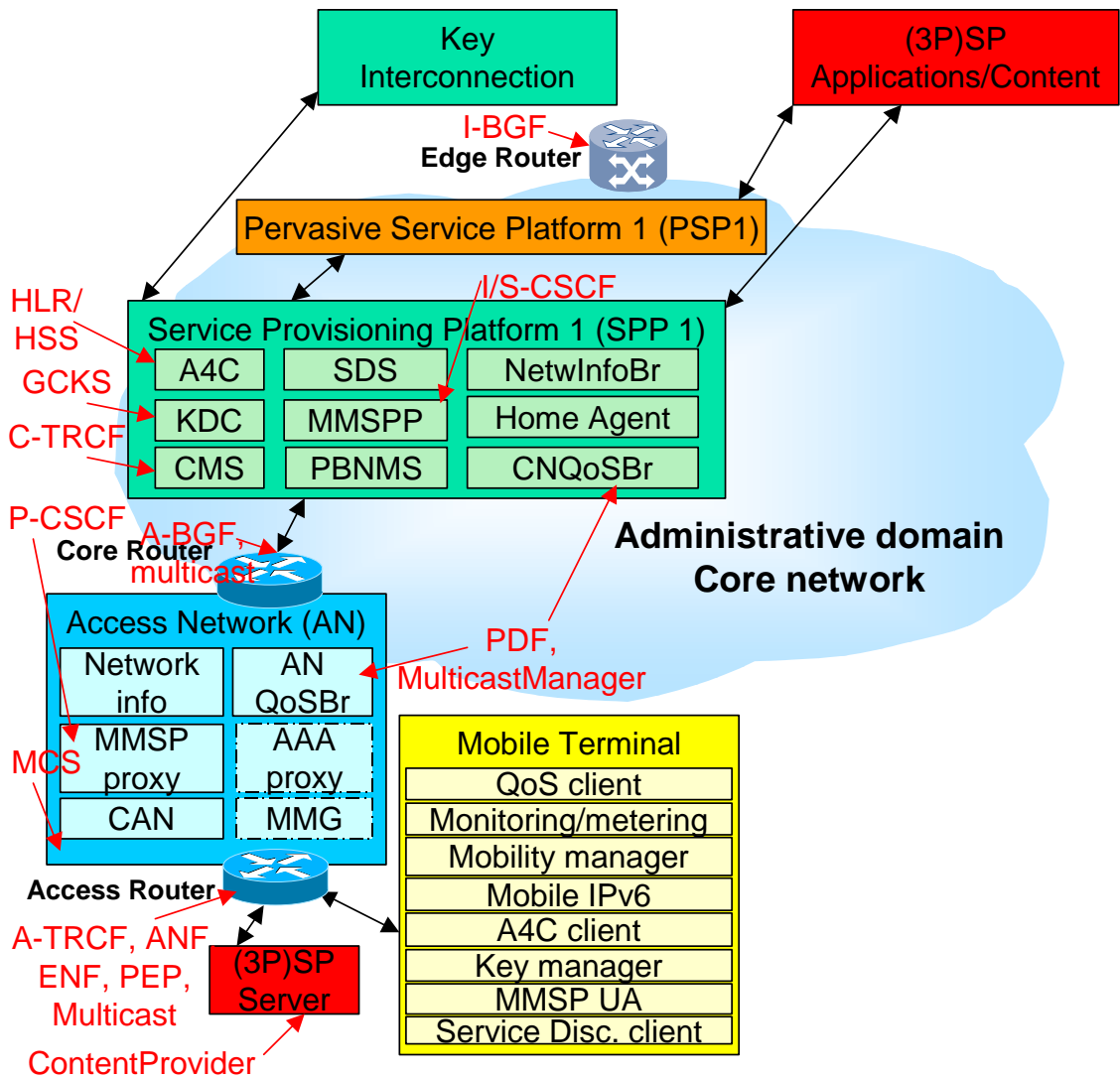


Figure 6 – Daidalos architecture with ITU and 3GPP terms

## 4.1 QoS aspects (session mobility & monitoring & Fast Handover)

### 4.1.i TISPAN

In Release 1 TISPAN supports nomadicty using Soft ISIMs and/or SIM cards. Handover between different access network types will be covered in later releases.

### 4.1.ii Daidalos

Main QoS aspects in Daidalos:

- In Daidalos QoS reservations can be done via the QoSClient in the terminal for legacy services and from within the network by the MMSPP or ARM for multimedia sessions.
- Monitoring is done at IP level (per flow and per DSCP) by a NetworkMonitoringEntity in each AccessRouter and for aggregates in each CoreRouter and EdgeRouter. This monitoring information is collected by CMS and used for both QoS measurements and Flow-based charging.

- Daidalos supports seamless mobility of terminals with Fast Handover within an administrative domain, and by a network-side single-sign-on mechanism across administrative domains
- Daidalos supports different types of mobility for multimedia sessions. It supports transferring active sessions from one MT to another, it supports transferring sessions to another user, and it will support transferring (parts of a) session to other active network interfaces.

## 4.2 Security & AAA (PANA)

### 4.2.i TISPAN

Many TISPAN security requirements for Release 1 are still unstable, and the result of the evaluation may change if the requirements are changed. A number of solutions is investigated (see table x).

Solution	Evaluation
IPsec/IKEv2	Requires support for IPsec, IKEv2, UDP encapsulation and an API for SIP application to modify security policies. May also need additional components, e.g. an application that modifies the MTU size for upper layer applications. The same IPsec implementation may be useful with other applications.
IPsec/SIP Digest AKA	Requires support for IPsec, SIP Digest AKA, and NAT traversal mechanism. If the UE is 3GPP compliant then support for IPsec and SIP Digest AKA is present but also a NAT traversal mechanism is needed. This means the 3GPP standard will not be applied as is in TISPAN.
TLS	Requires support for TLS. There is most likely other use for TLS than just protecting SIP, i.e. to secure HTTP or MSRP [MSRP, MSRP-RELAY]. Not clear if HTTP, MSRP and SIP can share the same TLS implementation.

### 4.2.ii Daidalos

Main functionality of security and AAA in Daidalos:

- Daidalos provides single sign-on for Network Access, Multimedia services (SIP) and Web Services using SAML. For network and multimedia access, SAML is transported in Diameter messages to the A4C server.
- PANA protocol (Protocol for carrying Authentication for Network Access) is used for network access which can be combined with datalink security like 802.1x mechanisms that use EAP

## 4.3 Broadcast/multicast

### 4.3.i TISPAN

TISPAN Release 1 does not yet take broadcasting into account. This is scheduled for Release 2 (beginning of 2007) or later.

#### **4.3.ii Daidalos**

##### **Main functionality of multicast/broadcast in Daidalos architecture:**

- Support for any source and multicasting of unicast streams
- Uni-directional downlink for DVB-H and MBMS
- Source driven QoS requests
- Joining via IGMP/MLD or via content provider
- Service can be offered at different qualities, user chooses quality depending on price, codecs, etc.
- Support for Access Network specific content adaptation
- Mobility Support for source and end-points
- Multicast data traffic can be IPsec-encrypted by the MulticastServer using Group Key Management (GKM) to enable (prepaid) charging.
- GKM is based on Logical Key Hierarchy (LKH) with Daidalos-specific (SAML-based) initial authorization phase.
- Reliable re-keying through the use of carouseling.

### **4.4 Multiparty calls**

#### **4.4.i TISPAN**

In TISPAN the CONF supplementary service is supported, both by emulation of this ISDN service, as by simulation through IMS SIP. When a UE invokes the CONF service, resources are allocated by a dedicated application server AS that enables the user to participate in and control a simultaneous communication involving a number of users.

#### **4.4.ii Daidalos**

Daidalos has a Content Adaptation Node (CAN) in each access network that support aggregation/mixing of audio/video. These CANs can be used to setup a multi-party call with audio, video and potentially other media. The first user will INVITE the CAN and will get a “302 MOVED” with a conference URI, and INVITES this. After this, the first user can INVITE others to join the session by sending a SIP REFER to those users with the conference URI.

## **5 Conclusions**

In this paper a brief comparison of the architectural approaches of ETSI TISPAN and the Daidalos project was given. In a number of areas there is a relation between the issues that TISPAN aims to standardize and the solutions that Daidalos investigates. Although Daidalos focuses more on the signaling and service aspects, while the access networks are assumed to be generic IPv6, and less attention is given to the support of legacy ISDN/PSTN services, in the area of QoS and mobility, security and AAA, broadcast/multicast and multiparty calls, Daidalos is proposing solutions that can be of potential interest to the TISPAN standardization work.

## 6 References

- [1] Draft ETSI ES 02007 TISPAN NGN Functional Architecture Release 1
- [2] Draft ETSI ES 02029 TISPAN NGN Functional Architecture Release 1 IP Multimedia Subsystem (IMS)
- [3] Draft ETSI DES 02019 TISPAN NGN Release 1: Functional architecture for PSTN/ISDN Emulation
- [4] Draft ETSI ES 02021 NGN Functional Architecture; Network Attachment Subsystem; Release 1
- [5] Draft ETSI ES 02020 NGN Functional Architecture; Resource and Admission Control Subsystem (RACS); Release 1
- [6] *3GPP TS 23.141 V6.2.0 (2003-03), "Presence Service – Architecture and Functional Description"*
- [7] Rui L. Aguiar, Dennis Bijwaard, Jurgen Jahnert, Paul Christ, Hans Einsiedler, "Designing Networks for the Delivery of Advanced Flexible Personal Services: the Daidalos approach", in Proceedings of IST Mobile & Wireless Communications Summit 2004, Lyon, France, June 2004
- [8] D. Bijwaard et al, Daidalos deliverable D311: Initial Network Architecture Design and sub-Systems Interoperation, 2004.
- [9] S. Sargento et al, "Daidalos Deliverable D321, QoS Architecture and Protocol Design Specification.", 2004.
- [10] A.F.G. Skarmeta et al, Daidalos Deliverable D331 – "Security Framework Design Specification", 2004
- [11] Hasan et al, Daidalos Deliverable D341 – "A4C Framework Design Specification", 2004
- [12] R. Roque et al, Daidalos Deliverable D351 "*Service Creation Platform Design Specification*", 2004.
- [13] D. Bijwaard et al, Daidalos deliverable D312: Network Architecture Design and Sub-Systems Interoperation Specification, April 2005.