PERVASIVE SERVICES FOR NEXT GENERATION HETEROGENEOUS NETWORKS

Rui Aguiar[1], Dennis Bijwaard[2], Babak A. Farshchian[3], Karl Jonas[4], Amardeo Sarma[5]

[1] Instituto de Telecomunicações, Universidade Aveiro, Portugal, ruilaa@det.ua.pt;
[2] Lucent Technologies, Bell Labs Europe, The Netherlands, bijwaard@lucent.com;
[3] Telenor R&D, Norway, babak.farshchian@telenor.com;
[4] Fraunhofer Fokus, Germany, karl.jonas@ieee.org'
[5] NEC Network Laboratories, Germany, sarma@netlab.nec.de

Keywords: mobility, virtual identities, pervasiveness, broadcast, federation

Abstract

The overall goal of the European collaborative project Daidalos is to design, develop and validate a framework for next generation mobility-enabled networks. Envisioned scenarios include heterogeneous access networks, while requiring ubiquitous, services of adequate quality, broadcast integration, as well as the ability to support privacy and anonymity while making life easier for the end-user. This paper introduces the *five key concepts* of the EU IST project *Daidalos* and how these address such diverse challenges, and sketches achievements so far.

1 Introduction

This Daidalos framework supports the provisioning of secure, personalized and pervasive services that operate in a heterogeneous network and service environment. The envisioned scenario features heterogeneous access networks covering several generations of networks, while requiring ubiquitous, end-to-end services of adequate quality to be delivered. The heterogeneity should support fixed, mobile and broadcast (FMBC) convergence.

The mobile user is to be provided with seamless and pervasive access to content, services and networks at different locations with different devices. It is essential to support privacy and anonymity according to the user's wishes while making life easier for the end-user at the same time, such as by understanding the context of the user's environment. The use of context information for the personalization of services will be supported. While the expected landscape should be open from a business point of view covering several large operators as well as a large number of niche providers, access for the user must be made easy. He or she should not need to have more than a minimum number of business relationships. Daidalos is fully Internet / IP (v6) based.

2 Daidalos Architecture and Five Key Concepts

There is a lot of related work in the future networks area. 3GPP aims to evolve the 3G network to an All-IP network concept, but does not address pervasiveness, broadcast and universal identity concepts. The IETF addresses several protocols that solve some issues addressed above, but does not provide an overall architecture. Some EU projects, such as Ambient Networks, take a network centric view, while not integrating their networking concepts with overall service needs of the user. On the other hand, other projects are even more specialized. For instance, the EU IST MAGNET Project focuses on personal networking, while others are primarily concerned with security aspects, such as the PRIME project.

We believe Daidalos is the first project developing a comprehensive solution for the future scenario described above, covering several layers and viewpoints and making services easy and pervasive for the user. It will:

- Provide mobile users with an optimal and seamless access to networks and services everywhere,
- Support easy use while allowing control over how visible, reachable or anonymous he or she is,
- Make services and networks ubiquitous and seamlessly usable,
- Include broadcast seamlessly in relevant service or network offerings,
- Allowing players to participate in business and offer even niche services in a very dynamic way.

Daidalos addresses the significant technology gap to be bridged to meet customer needs and open new business opportunities and covers three dimensions: the network, the service provisioning and pervasiveness. The Daidalos five key concepts are at the core of the project to address the listed shortcomings:

1. *MARQS* – Mobility Management, AAA, Resource Management, Quality of Service and Security: Make network usage transparent despite heterogeneity, providing authorized users seamless access. The solution must at least be on par with existing solutions, such as at 3GPP, while offering flexibility and openness.

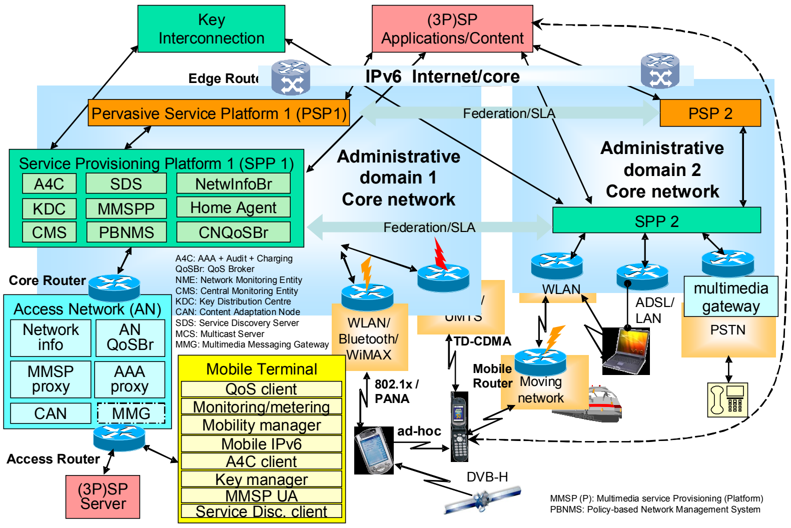
2. *VID* – Virtual Identities: Make users independent of their own or public devices, support privacy and the provision of services to users independent of what device they use and whether they own them. Such VIDs are assigned to a user independent of a specific device and contain the profile of services and networks used and may be used for pseudonymous access.

3. *USP* – Ubiquitous and Seamless Pervasiveness: Make services, networks and content ubiquitous and seamless. USP enables pervasiveness across fixed, portable and embedded devices and adapts to changing contexts and movement, as well as user requests.

4. *SIB* – Seamless Integration of Broadcast: Integrate entertainment, such as via TV or radio services, with information and communication services. Integration is needed at both the service level, e.g. for movies, and at technology levels, e.g. integrating DVB and WLAN, to separate the concern of *what* will be delivered from *how* it will be delivered.

5. *Federation*: Enable business players to enter and leave an area of business in a dynamic manner, such as to offer a new network, a new network service or a new information service or content, and cater for both existing and new, large and small network operators and service providers. Such a flexible business environment on the whole will benefit all, incumbents and newcomers, whether large or small.

Figure 1 below shows the Daidalos architecture, which has embedded the five key concepts at different levels in its components. The modules and functions indicated are now, at the end of the first phase of the Daidalos project, available as detailed specifications of modules and interfaces. The Daidalos network supports several access network technologies, and the Daidalos service provisioning platform includes SIP services on which the pervasive service platform builds. In contrast to 3G networks, *Daidalos is a pure IP solution*, with routers and servers replacing or complementing specialized 3G equipment.



A4C:	AAA + Auditing + Charging
AAA:	Authentication, Authorization, Accounting
QoSB:	QoS Broker
NME	Network Monitoring Entity
CMS	Central Monitoring Entity
KDC:	Key Distribution Centre
CAN:	Content Adaptation Node
SDS:	Service Discovery Server
MCS:	Multicast Server
MMG:	Multicast Messaging Gateway

Figure 1: Daidalos Network and Service Architecture.

2.1 The MARQS concept

MARQS brings together 5 critical dimensions of ubiquitous networks, and extends the three-dimensional approach covering mobility, AAA and QoS of the predecessor project *Moby Dick*, while adding the dimensions resource management and security.

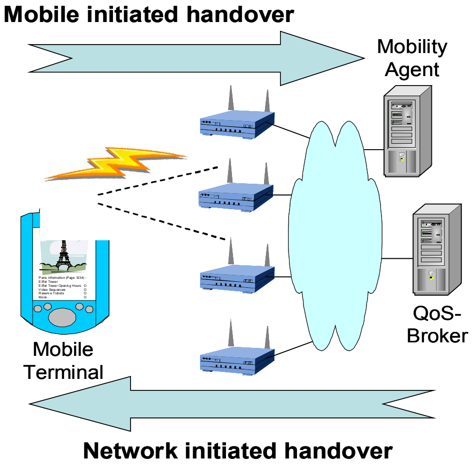


Figure 2: Mobile and network initiated handovers

Seamless mobility has been enhanced by improving fast handover to cover both terminal-initiated and network initiated handover. Handover by the network can be useful when it is required to balance load across access points, thus supporting *resource management*. Such handover covers several access technologies, and handover has been demonstrated for WLAN, Ethernet and TD-CDMA. Additionally, Daidalos 2 will look at integrating multi-homing to also support soft handover with more than one interface carrying data during the handover phase.

Quality of Service in Daidalos supports the negotiation and management of network resources at IP level for both legacy and multimedia services, while guaranteeing mobility.

For *security* and *A4C* (Authentication, Authorization, Accounting, Auditing and Charging), Daidalos has developed a flexible access control mechanism for the heterogeneous and mobility-enabled environment with accounting and charging mechanisms. This can be both session or flow-based, as well as pre- and post-paid.

The Daidalos network facilitates the provisioning of basic network services including multimedia through its platform that supports service discovery in addition. Content delivery to heterogeneous clients made possible using content adaptation schemes. Several flavors of mobility are thus supported, ranging from terminal via session to user mobility.

To discover the identities and capabilities of candidate Access Routers, Daidalos has specified and implemented the Candidate Access Router Discovery (CARD) protocol [5] and integrated this with functions that allow network-initiated fast handover based on performance measurements. Full QoS support at Layers 2 and 3 including the QoS mapping between the layers and for end-to-end delivery were specified and implemented. The Key Management infrastructure supports the Daidalos Security Architecture and provides flexible access for a heterogeneous and mobile environment. Current operational prototypes show power-up and registration followed by terminal-initiated or network-initiated handover supporting mobility.

2.2 Virtual Identities in Daidalos

Virtual identities (VIDs) are the Daidalos solution to the requirements to have flexible identity management and anonymity. VIDs separate users from their device and represent user-controlled user related attributes within the system. The flexible scheme supports both privacy and personalization. The VID contains a pseudonym together with additional information such as a profile, credentials and usage trace. A VID is a view that somebody in the system has on the user. Several VIDs can be associated with an operator subscription.

To enable authorization across domains with an ID-Token, a pseudonym is constructed from a unique identifier and the name of the home domain: identifier@domain. The ID-Token is a combination of the pseudonym and authentication information (see Figure 3) and is created by the SAML (Security Assertions Markup Language) authority, which enables the same authentication mechanism for both web and network services. The ID-Token contains the following elements:

- The *pseudonym* in plain text,
- Another part encrypted with receiver's public key, containing the following:
    - A *random number* to make the ID-token different each time it is sent.
    - A *sequence number* to avoid replay, which is checked by SAML Authority.
    - An *artifact* that references the appropriate SAML assertion referring to the subscription of the user with a network operator.
    - A *digital signature* using sender's private key via the ID-token excluding pseudonym

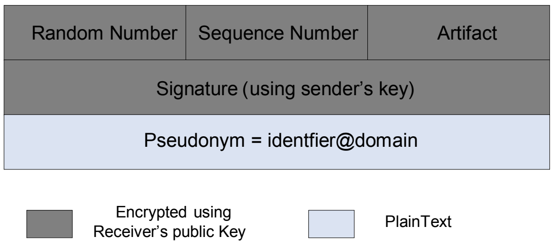

Random Number
Sequence Number
Artifact
Signature (using sender's key)
Pseudonym = identfier@domain
Encrypted using Receiver's public Key
PlainText

Figure 3: VID data structure

Different VIDs can be created to provide privacy by using an alternative name or pseudonym. The user has an option to make only part of its real identity available by revealing only the part needed for a service. A VID without any personal information can be used for anonymity. The VIDs can be used to access both basic services like Network Access and Multimedia Services, and more advanced services like (3rd party) applications.

To enforce privacy, it should be difficult, if not impossible to correlate VID usage of the same user. To ensure this the following measures are taken:

- Only one component in an operator domain holds the subscription information of users including the available VIDs in this subscription. This Daidalos component is the A4C (Authentication, Authorization, Accounting, Auditing and Charging) server, which includes the SAML authority.
- The user has a secured store, from which he can select VIDs to use. From this store, the user can select a VID to use for a certain service.
- By limiting the accessible user information in the different VIDs and making this information disjoint, the user can make it more difficult for third parties to correlate VIDs.
- The user presents an IDToken with a certain VID to the service he wants to use, and the service can check its validity with the A4C for authentication purposes.
- By referencing the pseudonym, attributes and profiles can be stored in a distributed manner (e.g. close to where they are used) without revealing the user's identity.

An open issue is to prevent correlation of VIDs from information in the communication layers, such as IP or MAC addresses. Another is the usage of the VID in combination with web service subscriptions.

2.3 Bringing Pervasiveness to Networks

Daidalos is filling an important gap in pervasive computing research and development. Traditional pervasive computing research has focused on user interaction aspects of pervasive computing, such as proper design of applications and devices that considers psychological and sociological aspects. Daidalos is building on this important research, and adds scalability.

Adapting services to user needs requires knowledge about the user in the form of preference and context information. This information is typically collected through a heterogeneous technological infrastructure, and is represented in various formats. The information can be used for the provisioning of services as well as to help the user select or optimize the service. Context information affects not only single services, such as those residing on the various devices the user is using, but also influences the whole process of discovery, selection and composition of advanced services. Due to the dynamic context of the user, changing rapidly and in unpredicted ways, a composed service will have to adapt dynamically and will have to continuously reconfigure itself. This adaptation can be a source of information for better personalization and adaptation to user preferences.

The picture is even more complex when considering the huge number of users and providers related to telecommunication systems. Each user will have his or her individual needs and will require a specific configuration of network resources and services. Each user will access the telecommunication network through a variety of network-enabled devices connected to the network through heterogeneous access technologies with varying quality, security, etc. The services in a pervasive environment will be provided by a large number of providers, raising the issue of privacy and the social and legal issues connected to it.

Putting users into focus brings fundamental challenges. Daidalos is unique in that it integrates services, including 3rd party services, into the combined network and service infrastructure. Traditional network architectures are indifferent about user contexts and needs, and often divide the service layer from the lower network layers. Services become pervasive through a personalized and adaptable network.

Based on the assumption that a magnitude of services will be available everywhere in a personalized manner, Daidalos divides pervasiveness into two interrelated areas of functionality:

- *Everywhere access to services*: The service that a user subscribes to or wants to use has to be available to the user when it is needed regardless of network technology, device technology, service type or user location. This is done in close interaction with device and user mobility, AAA, QoS and security. The Daidalos project has paid particular attention to scalability, user identity and privacy covering any device anywhere in the network. The Daidalos architecture supports discovery and composition of services and session management.
- *Context-aware access to services and access to context*: Not only should services be accessible everywhere, they should also be customized to the user's context and preferences. The Daidalos project is developing mechanisms for collecting relevant information from the network infrastructure, sensors and services. APIs support 3rd party applications that can access and provide information in a controlled manner. This way, Daidalos platforms become enablers for service providers, as they can context-enable their services and provide additional context. Quality-assurance of this raw context information and its refinement into accurate and suitable information for services is central to Daidalos.

An overall architecture for the pervasive service platform is shown in Figure 4 below. It provides a set of APIs towards 3rd party service providers, which are mostly based on open but controlled web standards, and relate to the two areas of functionality described above. Service and Identity Management APIs provide functionality for VID management and personalization, service discovery and composition, dynamic session management and deployment. User Experience Management API provides access to functionality such as learning user preferences, negotiation of privacy when accessing services, and refined context provisioning. By adopting this layered approach Daidalos provides an attractive transition path to 3rd party service providers who have already invested in web standards.

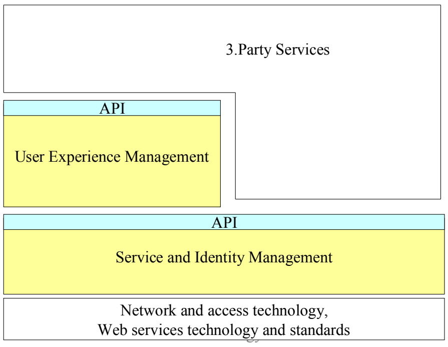

3.Party Services
API
User Experience Management
API
Service and Identity Management
Network and access technology,
Web services technology and standards

Figure 4: Overall service and network architecture

As a comprehensive approach covering several layers, the network in Daidalos supports pervasive services by providing network-level context, such as on availability or even geographic position. This enables the user has to access an abstracted network context that helps him or her to make appropriate network and service choices. Plans for the second phase of the project include integrating and providing sensor, terminal and network based context information. These can trigger or support resource management or initiate and change multimedia sessions. Such information could also be used to reduce or enlarge charges, such as by noting that someone is close to a billboard.

2.4 Broadcast Integration

A seamless integration of broadcast functionality into an overall communication environment has to take multiple aspects into account, in particular:

- full integration of broadcast radio, allowing both users and service providers to take advantage of specifics of broadcast technologies without having to consider the underlying technology (as far as possible);
- support for point-to-multipoint transmission in the network layer, to mimic the capabilities of traditional broadcast networks in every environment;
- provisioning of well-known broadcast services (such as TV or carousel) independent of the underlying communication network.

We have addressed the broadcast modes of multiple radio technologies, specifically W-CDMA (MBMS), WiMax (IEEE 802.16), WiFi (IEEE 802.11), DVB-T, -H, and DVB-S. Each has very specific capabilities that need specific treatment to enable seamless integration.

- For W-CDMA, a radio access point with direct IPv6 interface had been developed in one of the predecessor projects. Here, broadcast capabilities of the MBMS are added to the prototype and the mapping of IP multicast to broadcast bearers was developed.
- In WiMax and WiFi, the multicast channel at the radio layer imposes specific limitations such as reduced bandwidth that needs to be taken into account, in particular by the QoS management.
- DVB-T – and usually DVB-S – is unidirectional by nature. This has multiple implications, such as the requirement to provide a virtual return channel based on unidirectional link routing, leading to additional requirements to the mobility system, QoS, and A4C, and the need to cater for the unavailability of a return channel.

Broadcast radio networks are typically used to provide point-to-multipoint services. Therefore, multicast communication has to be provided by the communication layers. New requirements on the multicast protocols for the seamless integration of broadcast include seamless handover for multicast groups, including inter-technology handover, local repair to cope with variations on the different radio links, and support for temporary unavailability of a return channel due to the support for mobile environments and even mobile networks.

Daidalos has included high-level services that are traditionally only provided in the radio part of broadcast networks to the IPv6 based network, and. The Daidalos project has developed mechanisms for dynamic modification of the transmission mode (Unicast vs. multicast), the guaranteeing of appropriate QoS, and the adaptation of broadcast content for some fraction of the receiving user group. The latter supports many users wanting to receive a soccer video at the same time, but only some of them are willing to pay for the HDTV version.

2.5 Federation

Daidalos strongly relies on Federation concepts. Daidalos business approach allows for a multitude of business roles: network providers, service providers, aggregators and platform providers as depicted in Fig. 5. In a real environment, these functional roles may be covered by different companies. Different business scenarios can be described by presenting different interrelationships (like ownership) between these roles, from monolithic operators that execute most of these roles to small micro-operators that provide only network access and rely on other operators for other functions. In Daidalos, the federation concept is the glue for this flexibility of scenarios.

Daidalos defines ‘federation’ as the existence of a trust and responsibility delegation between different entities in the network. These may be different parts of the same operator infrastructure, or parts under the administrative ownership of different operators. One example of the former is the management delegation that exists between an Authentication server (A4C) and a network manager (QoS Broker), where the server trusts the manager to perform the network-level control functions required for a specific user, as registered in the authentication server. Daidalos assumes this type of trust relationships exist between the equipments owned by the same operator – and naturally a secure management infrastructure should be in place to assure this.

Of more interest to the dynamic business scenario envisaged by Daidalos is to facilitate the exchange of exchange trust and responsibility between different administrative entities. This leads to a *horizontalization* of service provisioning (Fig. 5) with several categories of providers, such as access operators, core operators and service aggregators including mobile virtual operators, Value-added Service providers (VAS) and Content/ Value-addes Service Providers (CVASP). These providers will specialize in their specific markets, and establish service relationships with complementary operators, in order to be able to provide a complete service solution for their customers. With a service negotiation infrastructure in place, this environment can be fairly dynamic, providing facilities for the operators to exploit market competition to reduce total costs. A reliable trust infrastructure has to be in place – potentially by an independent, federated, operator – including Key Distribution Mechanisms, and Service Discovery Servers.

In general, federation does not mean the exchange of all information or control, but simply the essential elements required for an integrated service solution across operators to be provided to that user, in that context. Bringing pervasive services into play means that even more information has to be shared (user context, existing communication contracts, etc.), and a truly cooperative environment will be required between different potentially types of operators and service providers.

Regarding peering agreements, such as those used to enable roaming support, Daidalos users will be able to handover their network connectivity and sessions across operators given the existence of adequate federation agreements between those operators. These handovers will necessarily be slower in execution, given the required inter-operator trust checks, but can be often prepared in advance, and thus, in the Daidalos concept, can be realized for real-time communications.

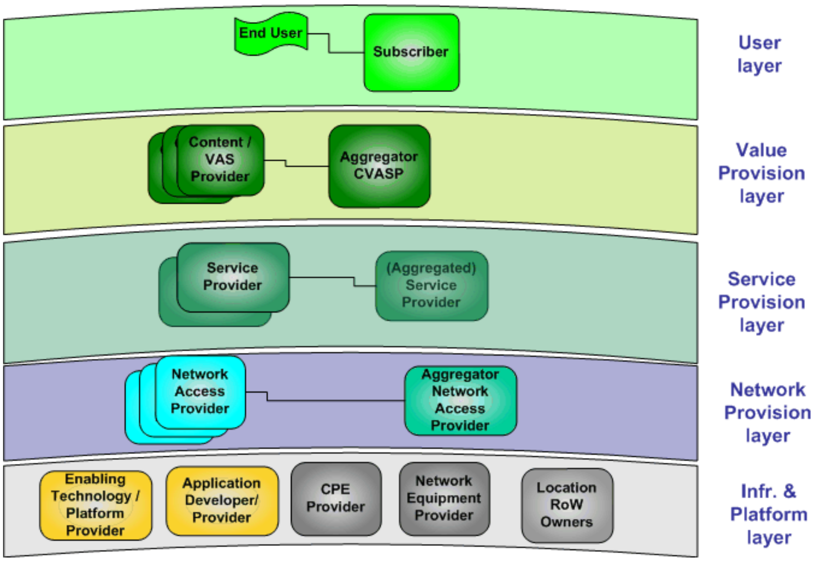


Figure 5: Overall service and network architecture

3 Validating the Daidalos Approach via Modeling, Simulations and Prototypes

There has been a multi-thronged approach in Daidalos to validate the concepts being developed. Overall Modeling serves to support overall completeness and consistency, including functional robustness. Simulations have been done in specific areas to validate specific concepts. Partial prototypes have demonstrated the viability of combining certain sets of functional and physical entities. Finally, the overall "Nidaros" prototype illustrates Daidalos as a whole using specific future scenarios.

3.1 Modeling

Daidalos has chosen a modeling approach to deal with the complexity of the system. One of the achievements of the project was to cover all part of Daidalos in an overall UML model that links the various parts to each other. UML models are also available for the components of the architecture, with some parts already modeled to state-machine or message sequence chart level. These have so far served to check in particular the completeness and consistency of interfaces, which is very important in view of the integrated demonstrators. The Daidalos project is currently putting the emphasis on the validation aspects of modeling.

3.2 Validations via simulations and partial prototypes

Simulations have in particular been carried out for specific items, such as paging for mobility and for QoS optimization. In addition, several subsystems have been prototyped and demonstrated for networking, services and pervasiveness. Examples are to validate network-initiated handover, moving networks and the pervasive services concept. Many of these results have been published elsewhere.

3.3 Status of overall "Nidaros" prototyping

The Daidalos concepts as a whole have been instantiated in a prototype test bed that should both provide a development platform for the technical work in the project, as well as to have an infrastructure to validate and assess innovations based on user-centric scenarios. These futuristic scenarios demonstrate user activities in a "Daidalos-enabled network". These scenarios cumulatively led to the setup of a validation environment, nicknamed "Nidaros". The user of the test bed perceives the Nidaros infrastructure in terms of the provided end-user services, since the Daidalos ambition is to keep the whole telecommunication infrastructure ubiquitous and transparent. In Nidaros, the user can access newscast services, video stream services, buddy finders, or videoconferencing facilities. The fairly complex test bed is schematically presented in Figure 6. Most Daidalos developments are already integrated in the test bed, and all major subsystems are now able to run independently.

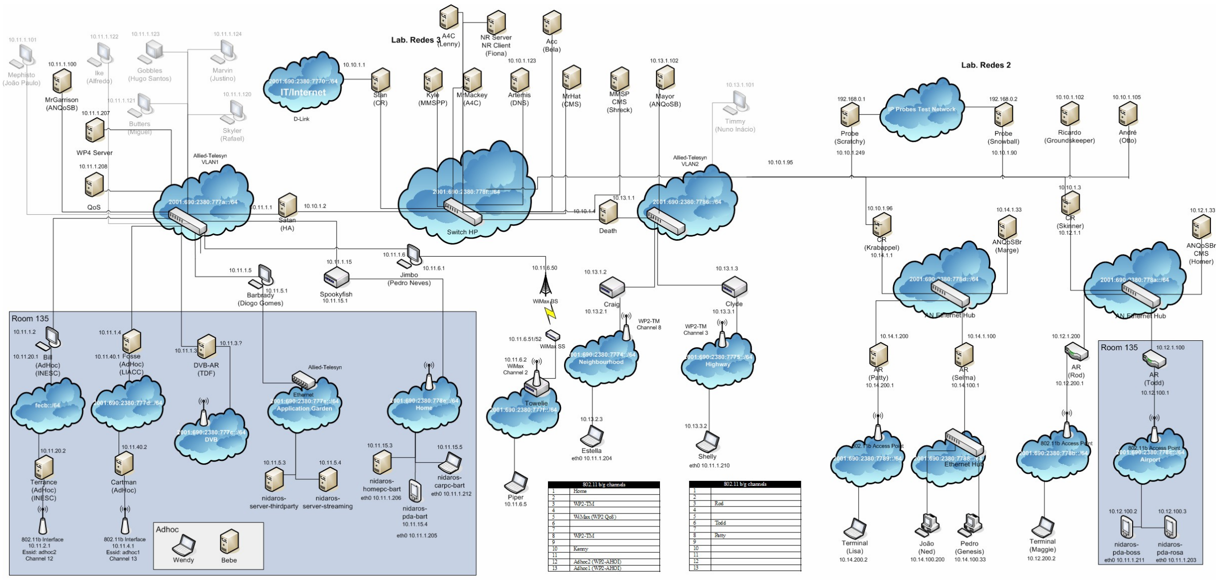


Figure 6: Overall service and network architecture

4 Summary and future work

This paper presented the Daidalos project and its key concepts for next generation mobile networks covering design and implementation decisions, and the validation by modeling and integrated prototypes. Highlights are the achievements for the key concepts and the realization in the integrated test bed Nidaros.

More research will be necessary for each key concept and the further integration and validation of those concepts to fulfill the Daidalos overall goal. Many challenges remain to be addressed. The VID concept needs to be transparent across all layers and integrated with addressing and naming schemes. The federation concept needs to take into account administrative domains, access networks and service providers. Specific network capabilities must be enhanced without having to register and pay for each service independently. The seamlessness of broadcast needs attention. In mobility, integrating multi-homing and soft handovers using multiple interfaces will be a major focus. Modeling will be extended to integrate testing to identify and eliminate conceptual errors and interface problems at an early stage. Finally, Daidalos concepts raise new questions, as business models may be changed radically. Operators may find that their largest asset is managing their customer, not owning networks and services. The implications for existing and new players both inside and outside the conventional telecoms field raise exciting questions for Daidalos II.

References

[1] Daidalos Web Site: http://www.ist-daidalos.org

[2] R. Aguiar, H.J. Einsiedler, H.W. Bitzer, R. Pascotto, J. Jaehnert, A. Sanchez: *An Operator and Scenario Driven Integrated Project*, 13th IST Mobile and Wireless Communication Summit, Lyon, France, June 2004.

[3] R. Aguiar, D. Bijwaard, J. Jaehnert, P. Christ, H. Einsiedler: *Designing Networks for the Delivery of Advanced Flexible Personal Services: the Daidalos approach*. IST Mobile & Wireless Communications Summit, Lyon, France, June 2004.

[4] J. Clarke, S. Butler, S. Dempsey, M. Crotty, J. Brazil; C. Hauser, M. Neubauer, A.J. Blazic: *Challenges of Identity, Authentication, and Discovery Management in a Ubiquitous environment: The DAIDALOS perspective*. 7th Int. Symposium on Communications Interworking, Ottawa, Canada, Nov. 2004.

[5] M. Liebsch, A. Singh, et all, RFC 4066: Candidate Access Router Discovery (CARD), IETF Network Working Group, July 2005.

[6] M. Liebsch, X. Pérez, R. Schmitz, A. Sarma, J. Jaehnert, S. Tessier, M. Wetterwald, I. Soto: *Solutions for IPv6-based mobility in the EU project Moby Dick*, World Telecommunications Congress 2002, Paris, Sep. 2002.