
MUSE White Paper

FMC Support in Fixed Access Architecture

Identifier: White Paper FMC
Class: Report
Version: 1
Version Date: 06/12/2007
Distribution: Public

EXECUTIVE SUMMARY

One of the central goals of MUSE is to develop a Global System for Broadband (GSB) architecture that supports multi-service access. That architecture shall also support Fixed Mobile Convergence (FMC) and bridge some of the gaps that currently exist between fixed broadband networks and mobile networks.

This white paper presents the main points of the resulting FMC architecture. Companion documents to the present white paper are a description of the overall GSB architecture with additional, more detailed implementation choices [1], and dedicated white papers on business models [2], QoS [3] and AAA [4] in a GSB architecture

The current white paper is focused on the support of:

- *nomadism*, i.e., allowing broadband users to establish connectivity and use their services when away from their home (i.e. residential) network
- *mobility with session continuity*, i.e., nomadism with the added feature that established sessions are not dropped as the user relocates or is on the move,
- *roaming*, i.e., nomadism and mobility with session continuity even when the user is in, or moving into or out of, a visited network domain.

These features are supported in fixed networks as well as in mobile networks (in this paper equivalent with 3GPP and WiMAX mobile networks). Hence, the goal has been to support roaming across fixed and mobile networks. The interworking with mobile networks is a very important feature of the proposed architecture.

The recommendations on which the architecture has been built include:

Interworking with 3GPP in general

- Short term interworking based on I-WLAN (3GPP's interworking WLAN specification) for nomadic support.
- Longer term interworking based on Mobile IP (MIP) or by optimized and network assisted SIP signalling, for mobility with session continuity support is proposed. The latter targets SIP-based applications and provides continuous (seamless) mobility and privacy protection whereas the former is applicable also to non-SIP-based applications.

Authentication, Authorization and IP addressing

- Authentication in nomadic situations is based on EAP with a decorated NAI to indicate the visited network. Based on the NAI, the EAP messages are routed to the correct AAA server.
- After successful authentication, the terminal receives an IP address from the visited network through DHCP.

Mobile IP

- A Mobility Controller in the Network Service Provider domain to assist in making handover decisions taking into account the resource availability in the access.
- Preference for DS-MIPv6 and PMIPv6 over the other existing MIP flavours, because of their intrinsically good fit in the migration from IPv4 to IPv6 and (in case of DS-MIPv6) the scope for tighter integration with the IP layer for route optimization.

SIP-based mobility

- For SIP-based mobility the preferred solution is a network supported SIP controlled IP soft handover (a make-before-break handover scheme). It supports all types of mobility (Personal, Terminal, Session, Service mobility) which also includes for instance the support of mobility between different terminals. Additionally this solution facilitates mobility across operators' frontiers and service characteristics (e.g. add/remove media) can be changed during the mobility event.

Roaming

- Three types of roaming agreements are sufficient for FMC in an unbundled business environment. This is more than the single roaming agreement in current mobile roaming, but still manageable.
- MUSE has defined the architectural functions and interactions between different involved business roles to enable authentication and authorisation in the case of roaming between fixed and mobile networks. MUSE has also defined an External Policy Manager function in the policy framework that enables to exchange of policies between different providers for visiting users.

An overall issue with the studied and proposed solutions is complexity. Although mobile handset vendors are starting to move towards more open operating systems and implementations, the world of mobile networks is currently based on highly controlled architectures all the way from terminal to core network. This is not the case in the fixed network domain where in particular the terminals are much more open than mobile phones are now. Still, features like mobility with session continuity, especially if seamless handover is desired, put such tough requirements that they are very hard to meet without very controlled architectures and terminals. The FMC architecture solutions in this paper are steps in the direction of a more controlled architecture for converged fixed and mobile networks.

TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	2
TABLE OF CONTENTS.....	4
ABBREVIATIONS.....	5
REFERENCES.....	7
LIST OF CONTRIBUTORS.....	9
1 WHAT IS FMC?.....	10
1.1 Central definitions and terminology.....	11
1.2 The MUSE unbundled business model.....	12
2 FMC ARCHITECTURE.....	13
2.1 Nomadism and mobility in fixed networks.....	13
2.2 Interworking with 3GPP mobile networks.....	15
2.2.1 <i>Interworking relationships</i>	16
2.2.2 <i>I-WLAN as interworking solution for nomadism</i>	16
2.2.3 <i>I-WLAN for fixed network subscriber in mobile network</i>	16
2.2.4 <i>I-WLAN for mobile network subscriber in fixed network</i>	17
2.3 Interworking with WiMAX networks.....	18
2.4 Path towards session continuity in FMC scenarios.....	18
2.4.1 <i>Mobility mechanisms in 3GPP and WiMAX architectures</i>	19
2.4.2 <i>MIP as interworking solution for session continuity</i>	19
2.4.3 <i>Extensions to 3GPP release 6 architecture to support MIP</i>	20
2.4.4 <i>SIP-based mobility</i>	21
2.4.5 <i>SIP based mobility versus MIP</i>	22
3 ROAMING.....	23
4 CONCLUSIONS.....	25

ABBREVIATIONS

3GPP	3 rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
ANP	Sometimes used for "Access Network Provider", however NAP "Network Access Provider" is the term consistently used in MUSE and DSL Forum.
ASP	Application Service Provider
AKA	Authentication and Key Agreement
B2BUA	Back-To-Back User Agent (a.k.a. Session Border Function)
CP	Connectivity Provider
CP-h	Home CP
CP-v	Visited CP
CSN	Connectivity Service Network
CSCF	Call Session Control Function
C-BGF	Core Border Gateway Function
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DS-MIPv6	Dual Stack MIPv6
EAP	Extensible Authentication Protocol
EN	Edge Node
EPM	External Policy Management
FA	Foreign Agent
FMC	Fixed Mobile Convergence
FMIPv6	Fast MIPv6
GERAN	GSM/EDGE Radio Access Network
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GRX	GPRS Roaming eXchange
GSB	Global System for Broadband
GSM	Global System for Mobile Communications
HA	Home Agent
HMIP	Hierarchal MIP
HMIPv6	Hierarchal MIPv6
HO	Handover
HPLFN	Home PLFN
HSS	Home Subscriber Server
I-CSCF	Interrogating CSCF
IEEE	Institute of Electrical & Electronics Engineers
IMS	IP Multimedia Subsystem
IPSec	Internet Protocol Security
I-WLAN	Interworking WLAN
L2	Layer 2
L3	Layer 3
L4	Layer 4
LAN	Local Area Network
MC	Mobility Controller
MCP	Media Content Provider
MIP	Mobile IP
MIPv4	Mobile IP version 4
MIPv6	Mobile IP version 6
MS	Mobile Station
NAP	Network Access Provider

NAI	Network Access Identifier
NA(P)T	Network Address Port Translator
NPM	Network Policy Management
NSP	Network Service Provider
NSP-h	Home NSP
NSP-v	Visited NSP
PANA	Protocol carrying Authentication for Network Access
PCRF	Policy & Charging Rules Function
P-CSCF	Proxy CSCF
PDP	Policy Decision Point
PDG	Packet Data Gateway
PDN GW	Packet Data Network GateWay
PLFN	Public Land Fixed Network
PMA	Proxy Mobile Agent
PMIP	Proxy MIP
PMIPv4	PMIP version 4
PMIPv6	PMIP version 6
RC	Resource Controller
RFC	Request For Comments
RGW	Residential GateWay
RNP	Regional Network Provider
SAE	System Architecture Evolution
SBC	Session Border Controller
SC	Service Controller
S-CSCF	Serving CSCF
SGSN	Gateway GPRS Support Node
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SPM	Service Policy Management
TCP	Transport Control Protocol
TOA	Tunnel Outer Address
UMTS	Universal Mobile Telecommunications System
UPM	User Policy Management
UTRAN	UMTS Terrestrial Radio Access Network
VPLMN	Visited PLMN
WAG	Wireless Access Gateway
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless LAN

REFERENCES

- [1] MUSE Deliverable DTF1.9 “GSB Access network architecture”, December 2007.
- [2] MUSE White Paper “MUSE Business Model in BB Access”, April 2007.
- [3] MUSE White Paper “QoS en policy control”, December 2007
- [4] MUSE White Paper “AAA Framework and Solutions for Broadband Access”, December 2007
- [5] Technical Report DSL Forum TR-058 “Multi-Service Architecture & Framework Requirements”, September 2003.
- [6] MUSE Deliverable DTF1.6 “Access network architecture III”, November 2006.
- [7] MUSE Deliverable DTF1.8 “FMC Support in Fixed Access Architecture”, June 2007
- [8] H. Haverinen (Ed.) and J. Salowey (Ed.), “Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)”, RFC 4186, January 2006.
- [9] MUSE Deliverable DTF3.4 “Specification of a Multi-Service RGW with Multi-Provider Functionality”, November 2007.
- [10] J. Arkko and H. Haverinen, “Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)”, RFC 4187, January 2006.
- [11] 3GPP TS 23.401: “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution: GPRS enhancements for E-UTRAN-access; Release 8”.
- [12] 3GPP TS 23.402: “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution: Architecture enhancements for non-3GPP accesses; Release 8”.
- [13] 3GPP TS 23.234: “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System to Wireless Local Area Network (WLAN) interworking; System description; Release 7”.
- [14] 3GPP TS 24.234: “3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP System to Wireless Local Area Network (WLAN) interworking; WLAN User Equipment (WLAN UE) to network protocols; Stage 3 (Release 7)”.
- [15] C. Perkins (Ed.), “IP Mobility Support for IPv4”, RFC 3344, August 2002.
- [16] C. Perkins (Ed.), “IP Mobility Support for IPv4, revised”, draft-ietf-mip4-rfc3344bis-03 (work in progress), March 2007.

-
- [17] D. Johnson, C. Perkins, J. Arkko, “Mobility Support in IPv6”, RFC 3775, June 2004.
 - [18] Hesham Soliman (Ed.), “Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)”, draft-ietf-mip6-nemo-v4traversal-04.txt (work in progress), March 2007.
 - [19] K. Leung, G. Dommety, P. Yegani, K. Chowdhury, “Mobility Management using Proxy Mobile IPv4” (work in progress), January 2007.
 - [20] S. Gundavelli, V. Devarapalli, K. Chowdhury, and B. Patil, “Proxy Mobile IPv6”, draft-ietf-netlmm-proxymip6-00.txt (work in progress), April 2007.
 - [21] IEEE Std 802.11, IEEE Standard for Local and Metropolitan Area Networks— Specific requirements — Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.
 - [22] WiMAX Forum network architecture, Stage 2 & 3, release 1.0.0, March 2007.
 - [23] Q-T Nguyen-Voung, L. Fiat, and N. Agoulmine, “An Architecture for UMTS-WiMAX Interworking”, In proceedings of IEEE 1st International Conference on Broadband Convergence Networks (BcN) 2006, Vancouver, Canada, April 2006.
 - [24] K. Oberle et al., MobileSummit 2007, “Enhanced Methods for SIP based Session Mobility in a Converged Network”, July 2007
 - [25] K. Oberle et al., BroadbandEurope 2007, “Mobility Management in a converged network “at work””, December 2007

LIST OF CONTRIBUTORS

Pieter Nooren (editor)	Netherlands Organisation for Applied Scientific Research (TNO)
Bob Melander (editor)	Ericsson
Peter Vetter	Alcatel-Lucent
Karsten Oberle	Alcatel-Lucent
Govinda Rajan	Alcatel-Lucent
Gábor Kovács	Budapest University of Technology and Economics
Hans Mickelsson	Ericsson
Wei Zhao	Ericsson
Zere Ghebretensaé	Ericsson
Alex De Smedt	Thomson
Benoit Radier	France Telecom R&D
Joseph De Biasio	France Telecom R&D
Olivier Roussel	France Telecom R&D
Enrique Areizaga	Robotiker
Iñigo Pinilla	Robotiker
António Gamelas	Portugal Telecom Inovação
Mohit Thakur	Siemens
Leonardo Ferracci	Telecom Italia
Antonio J. Elizondo	Telefónica I+D
Arnoud N.R. van Neerbos	TNO
Mark Prins	TNO
Jan van Loon	TNO
Arkadiusz Sitek	Telecom Poland

2 WHAT IS FMC?

Fixed-mobile convergence has been a term frequently appearing in the telecommunications and networking business area in recent years. It has been given many meanings, ranging from the desire of combined mobile and fixed network operators to use one single transport infrastructure to simply let mobile network subscribers access Internet application services from their mobile phone terminals.

In this white paper, the meaning of fixed-mobile convergence is very end-user oriented. The solutions aimed for should make the fixed networks and the mobile networks appear to the end-user as one seamless network infrastructure. Many research and standardisation initiatives are addressing FMC. The studies of MUSE contribute to the global efforts on FMC by investigating the issues from a fixed network provider perspective. The unified FMC infrastructure should enable the end-users to access their services no matter if connectivity is provided by a mobile network or a fixed network and no matter if the end-users are located within the domain of their home mobile network or the domain of some visited network. A particular form of FMC includes a flexible wireless attachment to a fixed or mobile provider network via hotspot facility. Further, the mobility and session continuity provided by mobile networks should be extended to fixed networks. However, achieving truly seamless handover for mobility in the fixed network domain is only an ambition and not a strict requirement.

This is a very challenging goal since 3GPP mobile networks and fixed networks are designed quite differently. Complicating matters even further is the fact that the aimed-for MUSE architecture strives for a large degree of unbundling whereas the 3GPP mobile network domain seemingly continues to be quite bundled in its structure. For the case of WiMAX mobile networks the situation is quite different and it is striking how many similarities can be found in the WiMAX and MUSE network architectures.

The proposed solution for interworking with 3GPP mobile networks is in the short term by I-WLAN (3GPP's interworking WLAN specification) for nomadic support. In the longer term, interworking by Mobile IP (MIP), alternatively by optimized and network assisted SIP signalling, for mobility with session continuity support is proposed. The latter targets SIP-based applications and provides continuous (seamless) mobility and privacy protection whereas the former is applicable also to non-SIP-based applications.

As part of the work on mobility management, an analysis of handover performance for various MIP flavours and SIP solutions has been performed. In terms of MIP this has led to a proposal for use of a mobility controller together with MIP to make handover decisions network resource aware and shorten network movement delay. MUSE decided to not to propose yet another MIP variant, but to analyse the ones already considered by 3GPP or WiMAX. Of the studied MIP flavours, DS-MIPv6 and PMIPv6 are recommended, because of their built-in support for migration to IPv6. DS-MIPv6 also allows for tighter integration with IPv6 for route optimization.

Roaming is a common phenomenon in mobile networks. Unbundling is a common phenomenon in fixed networks, but not in mobile networks. The introduction of roaming in fixed networks therefore requires several adaptations. Most notably are the impact of roaming on authentication and authorization and the related assignment of IP addresses. Roaming also has impact on the way policy management shall be applied. Last but not least, roaming also has an impact on the way roaming agreements shall occur. In general the number of types of roaming agreements will be higher than in traditional mobile networks, but a limitation shall be put on the variation of the agreements in order to be feasible.

An overall issue with the studied and proposed solutions is complexity. The mobile networks world is based on highly controlled architectures all the way from terminal to core network. This is not the case in the fixed network domain where in particular the terminals are much more open than mobile phones are. Still, features like mobility with session continuity, especially if seamless handover is desired, put such tough requirements that they are very hard to meet without very controlled architectures and terminals. The FMC solutions in this paper are steps in the direction of a more controlled architecture.

2.1 Central definitions and terminology

In MUSE the following basic definitions have been chosen to be used when describing FMC. They are all based on existing definitions used in different standardisation bodies.

Nomadism: Ability of the user to change his network access point on moving; when changing the network access point, the user's service session is completely stopped and then started again, i.e., there is no session continuity or handover possible. It is assumed that normal usage pattern is that users shutdown their service session before moving to another access point. *(Definition from ETSI/TISPAN)*

Roaming: This is the ability of the users to access services according their user profile while moving outside of their subscribed home network, i.e. by using an access point of a visited network. This requires the ability of the user to get access in the visited network, the existence of an interface between home network and visited network, as well as a roaming agreement between the respective network operators. *(Definition from ETSI/TISPAN)*

Session Continuity: The ability of a user or terminal to change the network access point while maintaining the ongoing session. This may include a session break and resume, or a certain degree of service interruption or loss of data while changing to the new access point. *(Definition from ETSI/TISPAN)*

For sessions where session breaks are not allowed Continuous Mobility is used.

Continuous Mobility: The ability of a mobile user/terminal/network to change location while media streams are active. *(Definition from ITU-T)*

Figure 2-1 illustrates the relationship between the aforementioned definitions. As can be seen in the figure roaming is a business relation that has impact on all technical topics.

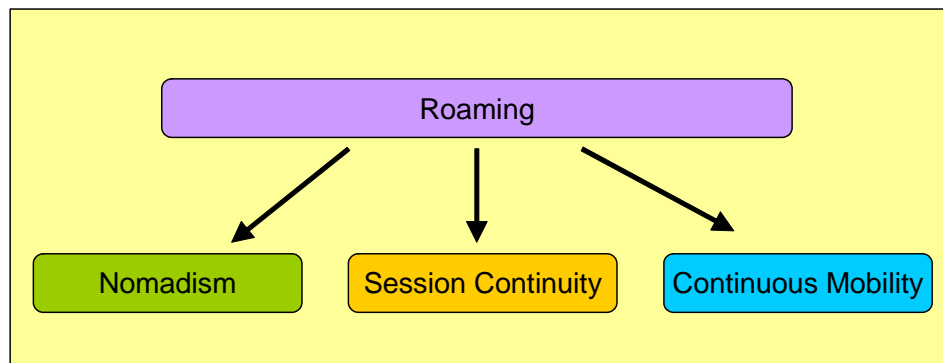


Figure 2-1: Illustration of relationship between definitions.

2.2 The MUSE unbundled business model

A major driving factor in the MUSE work has been the development of access network architectures suitable for multiple operators/service providers. This has led to the development of the highly decomposed business role model in Figure 2-2. The model is described in detail in a separate white paper [2]. The model is based on the DSL Forum model of TR-058 [5] with the addition of the Connectivity Provider and the Packager business roles.

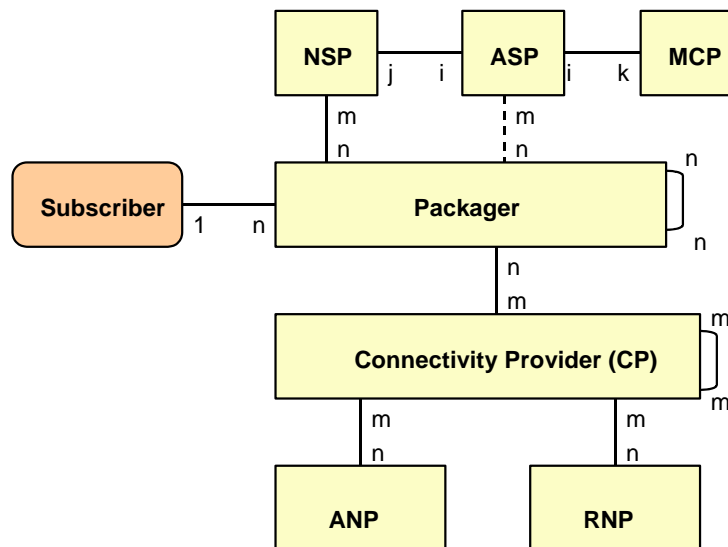


Figure 2-2: MUSE business role model.

In the figure, the various business roles are depicted together with their (potential) business relations. Several business roles in the model can be combined in real live business entities. Note that the Packager is the only business role that has a (business) contact with the Subscriber, but a Subscriber may have multiple Packagers (although he typically would have only one). The Packager then is responsible for the contracting of Connectivity Providers (CP), Network Service Providers (NSP) and Application Service Providers (ASP) in order to provide the required service to the Subscriber. The Connectivity Providers (there can be more than one for a given Subscriber) are then responsible for contracting the required Access Network Provider (NAP) and Regional Network Providers (RNP). In general, for a given location and a given access technique the Subscriber will have access to a single Access Network Provider and a single Connectivity Provider, but overall he may have access to more than one NAP and their associated CPs.

Since the Packager is the business role that has a business relation with the Subscriber it is the Packager that determines the home network of the Subscriber:

The home network consists of the networks of all NAPs, CPs, and NSP/ASPs that are (directly or indirectly) under contract by the Packager for the Subscriber. Note that this home network is different from the residential network that a subscriber may have in his home. Throughout this document, the term "home network" refers to the network determined by the Packager.

A Subscriber that is trying to access his services outside the network reach of these parties may have access to its services through a visited network. The parties operating the visited network must have roaming agreements with corresponding parties in the home network in order for the Subscriber to have access to its services in this situation.

3 FMC ARCHITECTURE

This chapter gives an overview of the functionality and procedures added to the MUSE architecture to support interworking with mobile networks. To that end the solutions are focusing on 3GPP and WiMAX type of mobile networks. Areas of the existing MUSE architecture that are affected by these changes are in particular the frameworks for AAA [4], IP address configuration, and policy control [3]. FMC also introduces two completely new areas to the fixed network domain: mobility management and roaming. Figure 3-1 shows the overall FMC enabled GSB architecture with the different functional blocks that allow for AAA, QoS, and session continuity.

3.1 Nomadism and mobility in fixed networks

A cornerstone of adding support for nomadism and mobility with session continuity in the fixed network domain is the ability to authenticate and enforce access control on a subscriber per terminal basis. In the non-nomadic/non-mobility case, only the RGW is authenticated and any number of users can reside behind that RGW (given that it supports NA(P)T). In case the residential subscriber, a guest, or a hotspot user wants to get access to a network provider different from the default network provider, another authentication is required with the network.

The evolved AAA solutions presented in MUSE Deliverable DTF1.8 [7] rely on the EAP framework. The EAP is used as a universal framework to carry different types of user credentials. The selected solutions are compatible with the general AAA methods for a GSB architecture, as described in more detail in a dedicated white paper [4]. They provide the means to separate visiting (i.e. nomadic or mobile) users from domestic users and to apply subscriber per terminal authentication to the former group even if both categories reside behind the same RGW. The solutions also allow for the authenticator and AAA client to be located in the AN, thereby removing the need for a trusted RGW. Hence, the extended functionality is hosted in the network nodes already used for AAA purposes (as indicated in Figure 3-1). From the fixed network perspective, any EAP method providing secure and mutual authentication is possible to use with those solutions. However, to facilitate interworking with 3GPP, EAP-SIM [8] or EAP-AKA [10] are required. There are different protocols that allow to carry EAP over the access network, each with their benefits and limitation (e.g. PPPoE, DHCP EAP, PANA, IEEE 802.1X), which are discussed in [4].

For *nomadic situations* when a user relocates and attaches the terminal to the network, either through a public WiFi hotspot or a hotspot in a RGW, it first performs EAP based authentication. Through the NAI (Network Address Identifier) of the subscriber, in roaming situations decorated to include the realm of the visited network, the EAP messages are routed to the correct AAA server. If authentication succeeds, the terminal is then configured with an IP address from the visited network using DHCP. The details are presented in MUSE Deliverable DTF1.8 [7]. The access provided to the terminal may be subject to policy enforcement and QoS provisioning as discussed in [7].

Two approaches for mobility with session continuity are proposed:

- 1) Implemented in network layer using MIP (Mobile IP)
- 2) Implemented in the application layer using SIP signalling.

For MIP based mobility the HA (Home Agent) for the fixed network subscribers is located in the Network Service Provider that provides the mobility service. In Figure 3-1 it is located in the node termed PDN GW (Packet Data Network GateWay to align with the 3GPP SAE terminology). Not all of the PDN GW responsibilities as specified in [11] are needed in a PDN GW in a fixed network NSP. Only the HA and functionality to support IP address configuration of MIP clients are guaranteed to be placed there.

There is also a MC (Mobility Controller) in the NSP that can be used to assist in making handover decisions that take into account resource availability in the access network. Depending on MIP flavour used the MIP client is either located on the terminal (client MIP, i.e., MIPv4 [15][16], MIPv6 [17], or DS-MIPv6[18]) or inside the network (PMIPv4 [19] and PMIPv6 [20]). When the MIP client resides in the network it is either located on the Access Node (AN) or the EN (Edge Node). Adhering again to 3GPP terminology the MIP client is then referred to as the PMA (Proxy Mobile Agent)[12]. In case there is MIPv4 FA (Foreign Agent) it is also located either on the AN or the EN¹. For PMIPv4 it is assumed that FA and PMA are collocated.

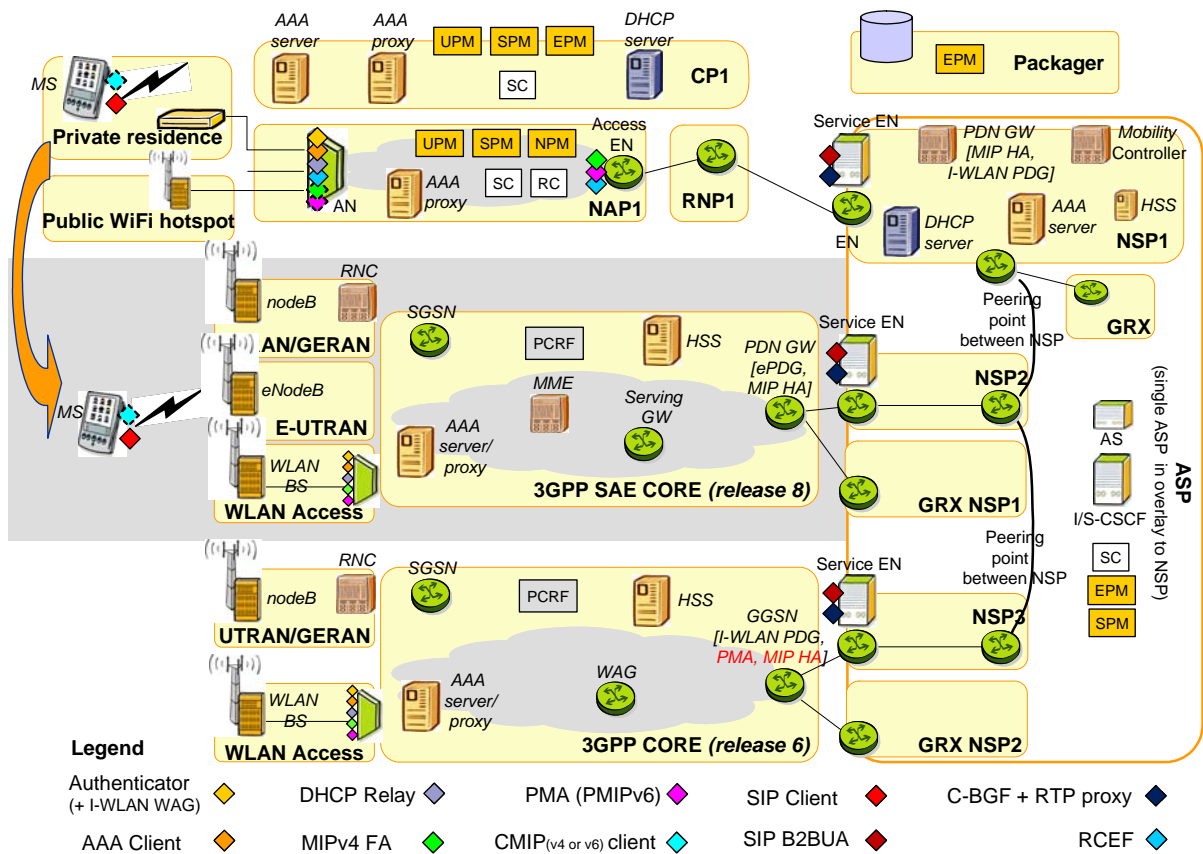


Figure 3-1: Node view of the MUSE FMC architecture with 3GPP release 6/8 network entities.

For SIP based mobility, there is a SIP client on the multi-homed terminal, and SIP B2BUA and C-BGF + RTP proxy in the service EN as well as some application layer functionality on the SIP Application Server in the ASP domain.

¹ The FA and the MIP client must be able to exchange datagrams without relying on standard IP routing mechanisms. This essentially means that no routers are allowed between FA and MIP client.

In scenarios with *mobility with session continuity* the user will attach the terminal to the network and perform authentication just as in nomadic situations. Configurations coupled to the mobility mechanism will then be initiated. For PMIP-based mobility the terminal will configure an IP address, the Ho@ (Home Address), again by means of DHCP. For client MIP, address configuration may include DHCP signalling to the terminal (MIPv4 CCoA, MIPv6, DS-MIPv6). The Ho@ is in that case configured using MIP signalling. For SIP-based mobility the terminal will configure an IP address using DHCP and then initiate the necessary SIP signalling. As the user relocates the mobility management mechanism will ensure that established sessions are maintained [7]. The approaches for MIP and SIP-based mobility are elaborated in section 3.4.

The UPM (User Policy Manager), SPM (Service Policy Manager), EPM (External Policy Manager), NPM (Network Policy Manager), Service Controller (SC) and Resource Controller (RC) are elements in the MUSE Policy Control Network elaborated in [7]. Especially the EPM function is important to exchange policies of visiting users between providers.

The FMC functions in the fixed and mobile networks from Figure 3-1 need to be complemented with functions in the Residential Gateway (RGW) in the subscriber's residential network and in the terminals. MUSE has developed a detailed specification for the RGW including FMC aspects [9]. For example, in a co-located hotspot configuration, an RGW at a subscriber's home provides access to both the subscriber himself and access to roaming visitors. The visitors can use the bandwidth that is left unused by the subscriber. In this co-located hotspot configuration, the RGW has a role in the authentication of the visitor and in the protection of the subscriber's services against traffic generated by the visitor.

3.2 Interworking with 3GPP mobile networks

The interworking with 3GPP mobile networks is achieved in two ways: one short-term solution based on I-WLAN [13] supporting nomadic use (and possibly also SIP-based session continuity) and one long-term solution relying on the upcoming 3GPP SAE (i.e., release 8) architecture [11][12] (or an extended 3GPP release 6 architecture) that will support MIP-based (and SIP-based) session continuity.

The I-WLAN solution facilitates interworking with 3GPP networks implementing release 6 of the 3GPP specifications. The deployment of the SAE solution likely lies several years away in time. The extensions to 3GPP release 6 also enables MIP-based session continuity but could likely be put to practice faster. It should be noted that the SAE architecture presented here is somewhat modified compared to the current release 8 specifications [11][12]. These modifications are proposed to improve the interfacing with the fixed network domain and are pinpointed in the subsections that follow (marked in red in the figures, as are the extensions to the release 6 architecture).

Figure 3-1 shows a node view of MUSE FMC architecture with the relevant fixed network and 3GPP network entities (extended release 6 and release 8) positioned in the architecture. The 3GPP entities are actually functional entities but they are here presented as physical nodes. In practice, such a mapping is not unlikely although different system manufacturers may decide to co-locate certain functions (e.g., Serving GW and PDN GW in one unit). The policy control entities in the figure (EPM, SPM, UPM, NPM, SC, RC and PCRF) are also functional entities.

3.2.1 Interworking relationships

The interworking between a fixed network and a 3GPP mobile network can take place between different business players through the means of roaming. The alternative is that one business player controls and operates both the 3GPP mobile network and a fixed network. Such combined operators are onwards treated as mobile centric in that their core network functions are assumed to conform to 3GPP specifications².

3.2.2 I-WLAN as interworking solution for nomadism

I-WLAN has been designed to provide interworking between 3GPP systems and other IP based access network (e.g., IEEE 802.11 WiFi [21] accesses). The interworking is *3GPP centric* in that the user subscription is assumed to be with a 3GPP mobile network provider. This is relaxed in the MUSE FMC architecture by allowing the user subscription to also be coupled to a fixed network provider.

For nomadic interworking using I-WLAN, the terminal, the fixed network and the 3GPP (release 6) mobile network need to support I-WLAN. In the fixed network, the WAG is preferably located in the AN (to keep the packet filtering enforcement close to the MS), the PDG (if one is used) is located in the NSP of the fixed network subscriber. That NSP may be required to peer with the 3GPP GRX backbone to make transport of AAA signalling possible for roaming situations between a fixed network domain and a 3GPP mobile domain. In Figure 3-1, the I-WLAN PDG is implemented in PDN GW node in the fixed network domain and collocated with the GGSN in the 3GPP mobile network domain.

3.2.3 I-WLAN for fixed network subscriber in mobile network

Since I-WLAN is 3GPP centric it does not need to cover native 3GPP radio accesses (GERAN and UTRAN). The home (and visited network in roaming situations) is supposed to be a 3GPP network so for GERAN and UTRAN accesses the normal 3GPP functionality is used. When subscribers of a fixed network only provider are introduced this changes, as there is no 3GPP core network functionality in the fixed network domain.

However, by implementing an HSS in the fixed network domain it is possible to allow for fixed network subscribers (with dual mode terminals) to use native the 3GPP RAN. The GTP tunnel (Gn) is then terminated in the GGSN in the *visited* 3GPP network³. The 3GPP specifications allow for this but in deployed 3GPP networks the Gn GTP tunnel is typically terminated in the GGSN in the home network.

² This assumption is indeed not always valid but it is made to reduce complexity and the number of cases necessary to discuss.

³ The user profile in the fixed network domain HSS could contain information that instructs the SGSN-v to terminate the GTP tunnel locally in GGSN-v. This information can be conveyed to the SGSN-v (and subsequently the GGSN-v) during (SIM/AKA) authentication.

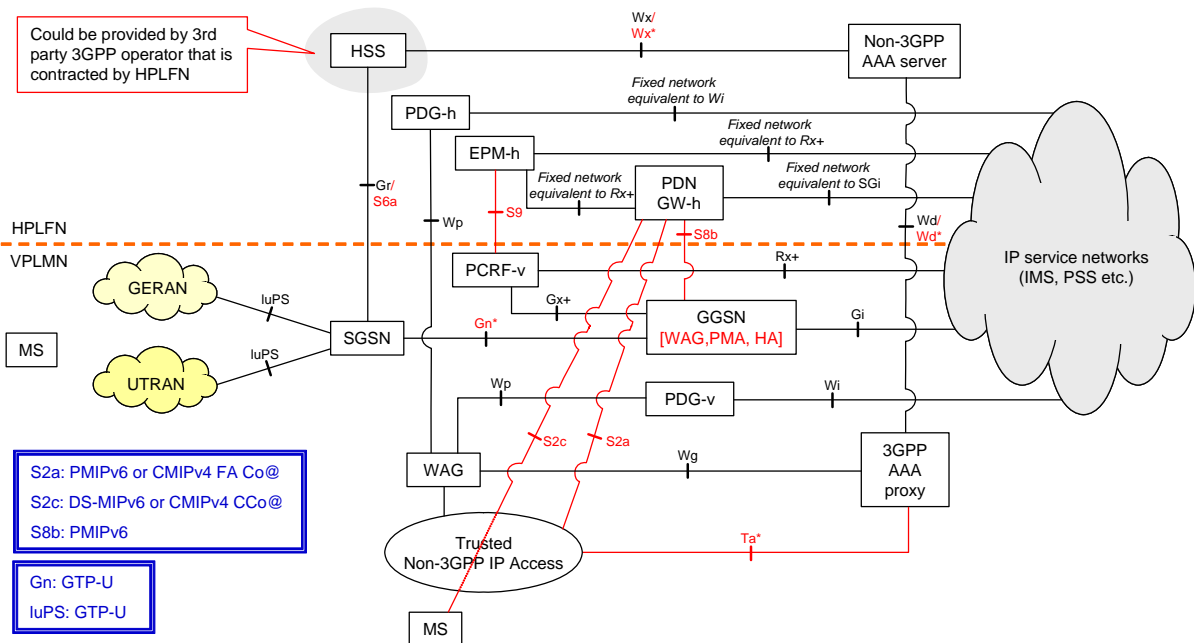


Figure 3-2: Functional view of the MUSE FMC architecture with 3GPP release 6 interworking when a fixed network subscriber is roaming in a 3GPP mobile network.

The visited network GGSN should also host a WAG. In this way packet filtering can be enforced if general or user specific policy require the fixed network user to tunnel its traffic to a PDG (either in the home fixed network domain or the visited 3GPP network domain⁴ – again dictated by policy). Figure 3-2 illustrates the relationships described above (the S2 and S8 reference points, the HA and PMA are extensions for MIP-based session continuity and are described in Section 3.4.2). Above the dashed orange line is shown the HPLFN (Home Public Land Fixed Network), a fixed network, and below the line is shown the VPLMN (Visited Public Land Mobile Network), a 3GPP mobile network (actually a combined mobile and fixed network since it also has non-3GPP accesses).

If the fixed network subscriber instead obtains connectivity from a non-3GPP IP access of a combined fixed and 3GPP network the regular I-WLAN procedures as specified by [13][14] are followed. If allowed by policy, the MS may use WLAN direct IP access. That is, use the local IP address in the non-3GPP IP access network obtained from the DHCP signalling that follows the EAP-SIM/AKA authentication. Otherwise, it must establish an IPsec tunnel to the PDG in the home fixed network domain or the visited 3GPP network domain (PDG-h and PDH-v, respectively, in Figure 3-2). In this case, the WAG will block all packets not belonging to the IPsec tunnel. This WAG is not necessarily collocated with the GGSN. It could be located closer to the non-3GPP access network. All of this is a direct application of the I-WLAN specification.

3.2.4 I-WLAN for mobile network subscriber in fixed network

This is a direct application of the I-WLAN specifications [13][14] and requires no further comments than what was discussed in the Section 3.2.3.

⁴ A PDG in the home network domain results in home network routed traffic, whereas the PDG in the visited network domain result in visited network routed traffic.

3.3 Interworking with WiMAX networks

Compared to 3GPP mobile networks, interworking with WiMAX mobile networks is considerably simpler from a fixed network and MUSE architecture perspective. The WiMAX network architecture [22] has many similarities with the MUSE architecture and the protocols and procedures used in WiMAX, e.g., for authentication and IP address allocation, are also largely the same.

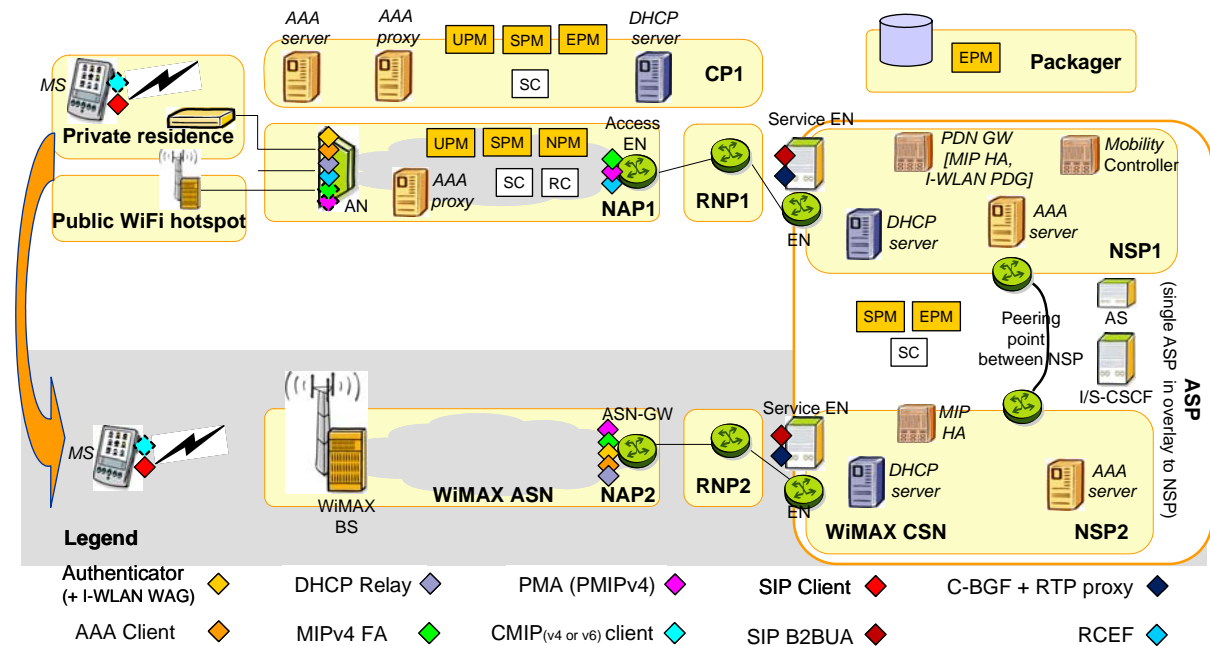


Figure 3-3: Node view of the MUSE FMC architecture with WiMAX network entities.

Figure 3-3 shows the WiMAX network nodes in the MUSE FMC architecture. The WiMAX (access network) hosts DHCP relay, authenticator, AAA client, and MIP functionality (MIPv4 FA and PMIPv4 PMA⁵). The MIP HA (for WiMAX subscribers) is located in the WiMAX CSN (Connectivity Service Network), which is operated by an NSP. The HA for the fixed network subscribers is located in the PDG GW of the NSP contracted by their Packager.

The many similarities with the MUSE architecture also means that the procedures outlined in Section 3.1 also apply to for the interworking with WiMAX mobile networks. That is, with regard to the MUSE FMC architecture, nomadism and mobility with session continuity across the fixed network and WiMAX domains is no different from nomadism and mobility with session continuity entirely within the fixed network domain. This is a very appealing aspect of the WiMAX architecture. Because of this similarity, interworking with WiMAX mobile networks is not discussed separately any further than this.

3.4 Path towards session continuity in FMC scenarios

Session continuity is often seen as an integral and necessary part of FMC and NGN in general. For interactive real-time multimedia services such as Voice over IP (VoIP) or Multimedia over IP (MMIP) it is clearly a necessity. For other services, it is recommended to apply a careful techno-economical analysis to confirm the requirement. This paper works from the assumption that there will be popular services for which session continuity is a requirement.

⁵ The WiMAX terminology for the PMA is PMIPv4 client.

3.4.1 Mobility mechanisms in 3GPP and WiMAX architectures

The many competing MIP alternatives that appear in the 3GPP and WiMAX architectures are an ominous cloud for the success of MIP as a basis for session continuity and interworking of fixed and mobile networks. The history of MIP has not been one of success when it comes to actual widespread deployment in the fixed network domain. Now that the mobile network world is embracing MIP it is therefore unfortunate that the embracing is done along such disparate paths. It will increase the complexity of nodes such as the PDN GW or GGSN. Risks that should not be underestimated are that the result will be yet another solution that does not make it from specification to actual deployment or that the solution will only work within limited “islands” of the network.

The MUSE recommendation is to use DS-MIPv6 and PMIPv6. There are two main reasons for this:

- The networking world is moving towards IPv6 (although the pace of change varies greatly among operators). A MIPv6 variant of MIP saves operators a cumbersome MIP migration on top of the already demanding IP migration. A MIPv6 variant requires that terminals (and HAs) are dual-stacked but this does not introduce complications as many modern OS (operating system) implementations have dual stack support.
- In addition, DS-MIPv6 also allows for tighter integration with IPv6, e.g. route optimization. DS-MIPv6 by definition is not restricted to IPv6 networks, but also supports co-existence with IPv4.

An issue with PMIPv4/v6 is how well it will work in practice with an “off the shelf” OS. On paper PMIP looks simple and requires no functionality on the MS. However, most likely the OS (the socket implementation) must be modified to tolerate the activations/deactivations of NICs (Network Interface Card) that will happen during mobility.

3.4.2 MIP as interworking solution for session continuity

Figure 3-4 shows the functional view of the FMC architecture in roaming scenarios based on 3GPP release 8. For MIP based mobility with session continuity the traffic is always home network routed. The figure is easily modified for non-roaming scenarios with only a combined 3GPP mobile network and fixed network operator. The HPLFN part then disappears, and all S2 reference points go to the PDN GW only (i.e., no S2 reference points with the Serving GW). In that case there is no S8b interface, only an S5 interface.

For completeness, Figure 3-4 shows ePDG nodes⁶ (in grey colour) in the 3GPP VPMLN. However, they will not be used in the MIP based solutions presented here since *a*) the fixed networks of the MUSE architecture enforce strong and secure authentication and access control and *b*) the ePDG complicates the mobility management and terminals. Hence, only trusted non-3GPP accesses are assumed, regardless if there is a roaming situation or not. In the presented solutions it is also assumed that for MIP mobility from non-3GPP accesses of a combined 3GPP mobile network and fixed network operator, S2 terminates directly in the PDN GW (i.e. no S2 reference points to Serving GW although they are, again for completeness, shown in the figure in grey colour).

⁶ According to 3GPP specifications an MS must establish an IPSec tunnel to the ePDG when obtaining connectivity from untrusted accesses.

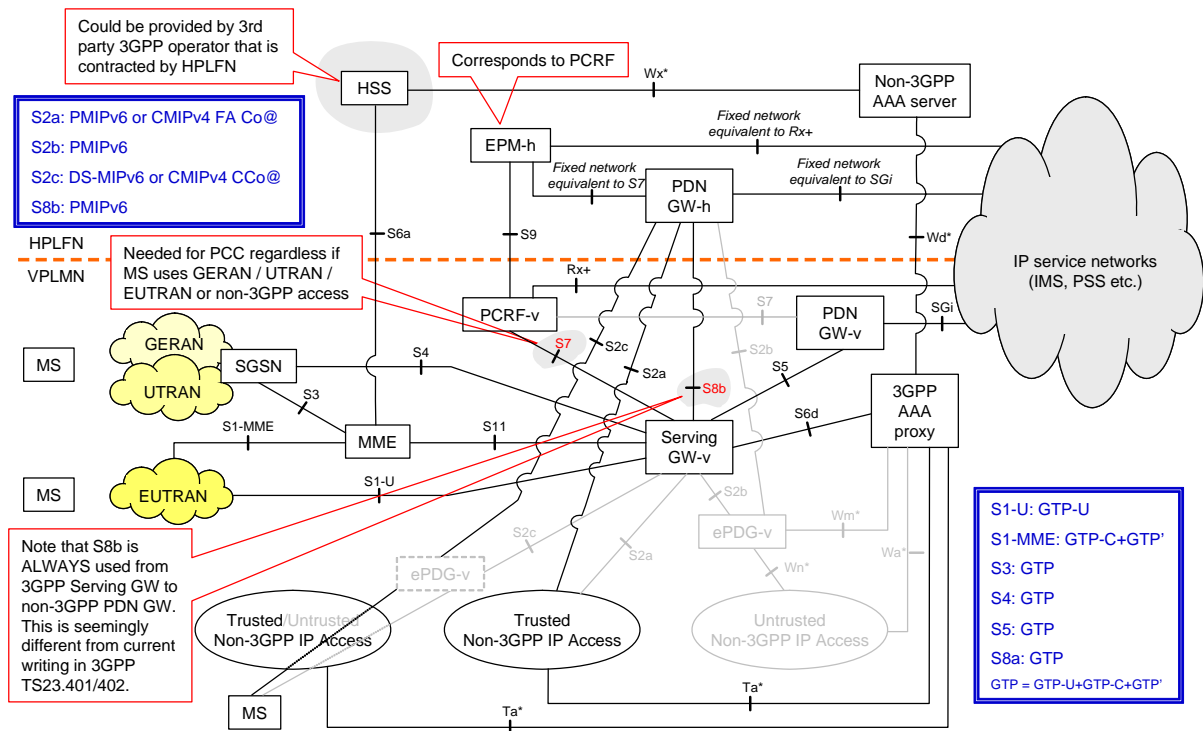


Figure 3-4: Functional view of the MUSE FMC architecture with 3GPP release 8 interworking when a fixed network subscriber is roaming in a 3GPP mobile network.

3.4.3 Extensions to 3GPP release 6 architecture to support MIP

So far the presentation here has only considered the upcoming 3GPP SAE architecture (release 8) for MIP based mobility and session continuity. It is however possible to extend the 3GPP release 6 architecture with MIP functionality that will enable it to function analogous to the SAE solution.

Figure 3-2 shows, marked in red, the extensions needed. The GGSN must implement a PMA and a HA. Similarly to the I-WLAN solution in Section 3.2.3, the Gn GTP tunnel is also here always terminated in the GGSN in the 3GPP network. For a fixed network subscriber the GTP tunnel is replaced in the GGSN by a PMIPv6 tunnel to the PDN GW in the fixed network domain (same as in the SAE-based solution although the tunnel switch there is done by the Serving GW).

During the 3GPP authentication procedure the SGSN learns from the user profile sent by the HSS that the subscriber needs special treatment. That is, the GTP tunnel should be terminated in the local GGSN in the 3GPP mobile network the fixed network subscriber is visiting. Then during the PDP context activation the SGSN informs that GGSN in the visited network that it should establish a PMIPv6 tunnel to the PDG GW in the home network. More details of the tunnelling are shown in [7]. A similar approach to this has been described in [23] but for MIPv4-based 3GPP interworking with WiMAX networks.

3.4.4 SIP-based mobility

During the last years, the SIP protocol has become the control protocol of choice that enables multimedia services. It also provides some means of mobility management. As an application layer solution it allows mobility to be managed on top of the IP layer, across boundaries between networks possibly managed by different operators. SIP offers several advantages in terms of mobility:

- facilitates mobility management across different operators' networks (multi-provider environment);
- is independent of the network access technology (support for heterogeneous access networks);
- is independent of the IP version;
- it is already established protocol for conversational services and incorporated by both ETSI TISPAN and 3GPP;
- supports all mobility types: personal, terminal, service and session;
- provides AAA functionalities: user/terminal identification and means to build the interface towards operators' AAA infrastructure.
- service characteristics (e.g. add/remove media) can be changed during the mobility event.

Apart from the advantages listed above SIP suffers from some shortcomings in the area of mobility management:

- Standard SIP session/terminal mobility methods (REFER and re-INVITE) are not able to provide continuous mobility. During the move to another IP address subnet, the SIP sessions (both signalling and data) are terminated because the underlying TCP/UDP socket addresses are no longer reachable.
- Due to the end-to-end nature of the SIP communications, privacy of the moving session/terminal can not be granted. Each time session/terminal changes IP address, this fact is signalled to the communication peer to redirect user data traffic to the new destination.

Within MUSE, an extended SIP-based mobility management solution has been developed to overcome issues derived from the standard SIP based mobility. The elaborated SIP-based mobility management solution does not require any new SIP method or header to be defined, but proposes novel access network architecture and functionalities. It is based on two concepts:

- IP Soft Handover - Allows seamless session transfer between terminal as well as terminal mobility applying a make-before-break handover scheme. It provides network support to the make-before-break handover process utilizing P-CSCF (SIP Back-to-Back User Agent) and C-BGF functions as well as RTP proxy and Conferencing module to allow seamless handover controlled at the SIP layer..... P-CSCF and C-BGF are sometimes combined into one node called SBC (Session Border Controller).
- SBC Daisy Chaining – when session/terminal moves from one network served by one SBC to another network served by different SBC, IP Soft Handover capable SBCs are daisy chained to provide seamless handover during such move.

Detailed description of the SIP-based mobility management solution for the FMC is given in [7], [24], [25].

3.4.5 Comparison of SIP and MIP based mobility

As already stated, MUSE considers both network layer and application layer mobility management methods to support Session Continuity and Continuous Mobility.

An analysis of the tests results from various literature sources [7] indicates that both network layer (MIP) and application layer (SIP) mobility management schemes provide Session Continuity, but with noticeable service interruption or loss of data while changing the network access point. Neither basic SIP nor basic MIP implementation (applying terminal driven handover) can provide Continuous Mobility. Both SIP and MIP provide comparable disruption time periods during handover, so it is not possible to point out a superior mobility management method (network layer vs. application layer) in terms of its performance. In both cases, the main part of the handover delay is caused by link layer handover, movement detection at the network layer, IP address acquisition and configuration. Authentication can also be a significant source of delay, especially if performed at many layers and without any coordination and optimization (e.g. IMS authentication is mandatory regardless if lower layers perform authentication). Both SIP and MIP message exchanges constitute only a minor part of the handover delay. MUSE has proposed enhancements to both SIP-based and MIP-based mobility management methods.

In case of the SIP based mobility, the SIP-controlled IP Soft Handover is capable to provide a continuous mobility. It requires SIP handover to be supported by means of SIP B2BUA and RTP proxy functionalities localized in the network edge (SBC). The SIP-controlled IP Soft Handover makes the network aware of an outgoing session transfer process. In terms of the terminal mobility the solution also requires mobile terminal to be able to operate two network interfaces at the same time (multi-homed terminals). The terminal must be able to anticipate change of the network attachment point, obtain new network interface configuration and signal change of the network layer and transport layer configuration while maintaining existing communication through "old" network attachment. SIP-controlled IP Soft Handover enhances make-before-break mechanism by means of the packets replication and filtering functions (RTP proxy) localized both in the network and multi-homed terminal (in case of the terminal mobility only) what provides the means to minimize a packet loss due to the move.

MIP is the protocol family of choice for inter-access mobility management in heterogeneous networks involving both 3GPP and WiMAX. It possesses multiple advantages in terms of mobility: it is transparent to applications and network agnostic. However, as performance results showed, it is not possible to assure seamless handover employing typical MIP configuration where the handover is entirely terminal driven. Consequently, some kind of network assistance during handover is needed to provide MIP-based seamless mobility. 3GPP is proposing Proxy MIPv6 to provide generic mobility service to legacy, non-MIP capable, terminals. PMIPv6 emulates the MN's home network while roaming. While the 3GPP solution is entirely mobile operator centric, MUSE has proposed a solution to allow fixed network subscriber to take advantage of the PMIP-based convergent mobility management. The solution requires HSS functionality to be either provided by the fixed operator itself or by a 3rd party 3GPP operator contracted by fixed network operator.

4 ROAMING

In the MUSE unbundled fixed-mobile architecture, roaming is an important aspect for the support of nomadism across administrative domains. Within MUSE it has been assumed (for simplicity reasons) that roaming implies session interrupt. This corresponds to today's situation with roaming in mobile networks. Note that one of the reasons for session interruption for roaming is the complexity arising from charging of existing sessions while moving across network boundaries.

Roaming requires the introduction of roaming agreements between visited business roles and home business roles. In mobile networks, such roaming agreements of course already exist, but the home and the visited networks are each operated by a single business entity. In fixed networks and perhaps in future fixed-mobile integrated networks roaming, agreements will involve multiple roles in the home network and multiple roles in the visited network. In theory, roaming agreements can be made between various parties in the home and visited network, such as between a CP-v and Packager-h, or between an ASP and NAP-v, etc. Such an arrangement would require each party to have a multitude of types of roaming agreements in addition to the ordinary business relations already existing in their own network.

An analysis by MUSE shows that it is sufficient to restrict the roaming agreements to parties of the same type. That is, roaming agreements need only exist between:

- CP-v and CP-h,
- NSP-v and NSP-h, and
- Packager-v and Packager-h

Roaming agreements between NAP-v and NAP-h (and between RNP-v and RNP-v) are usually not needed, because each NAP (and RNP) has usually only local significance and the associated CP can take care of the required roaming agreements. In Figure 4-1 the above observations are depicted.

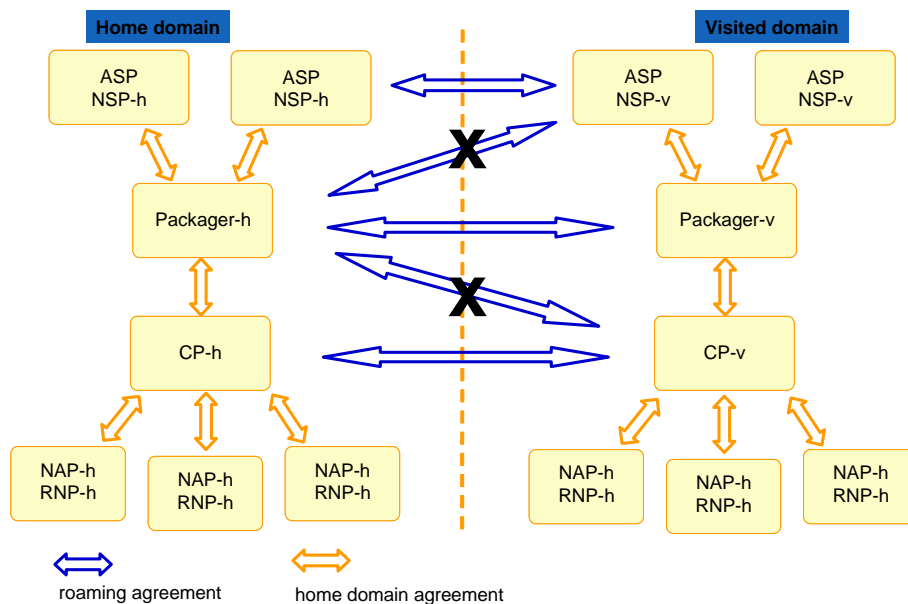


Figure 4-1: Three roaming agreement types needed in unbundled FMC environment.

From the above three types of roaming agreements, the agreements between CP-v and CP-h, and between NSP-v and NSP-h will occur the most frequently. Roaming agreements between Packager-h and Packager-v will occur only in special occasions when the standard roaming agreements between CPs and between NSPs are not sufficient.

5 CONCLUSIONS

One of the central goals of MUSE is to develop a Global System for Broadband (GSB) architecture that supports multi-service access. That architecture shall also support Fixed Mobile Convergence (FMC) and bridge some of the gaps that currently exist between fixed broadband networks and mobile networks.

This white paper presents the main points of the resulting FMC architecture that supports

- *nomadism*, i.e., allowing broadband users to establish connectivity and use their network services when away from their home (i.e. residential) network
- *mobility with session continuity*, i.e., nomadism with the added feature that established sessions are not dropped as the user relocates or is on the move,
- *roaming*, i.e., nomadism and mobility with session continuity even when the user is in, or moving into or out of, a visited network domain.

Understanding the implications of these three features and providing solutions for them in *fixed* networks has turned out to be a formidable task by itself. Adding to the complexity is the fact the 3GPP mobile architecture and the MUSE fixed network architecture are designed quite differently and do not share many architectural design choices. This is not the case for the WiMAX architecture and for this reason interworking with WiMAX has been considerably simpler from a MUSE architecture perspective. A final difficulty when it comes to 3GPP mobile networks is that the most recent 3GPP architecture being developed (and which particularly addresses convergence), the SAE (System Architecture Evolution) – release 8, has been undergoing continued revisions during the work in MUSE. The 3GPP mobile network architecture to interwork with has therefore been a “moving target”.

The recommendations on which the architecture has been built include:

Interworking with 3GPP in general

- Short term interworking based on I-WLAN (3GPP’s interworking WLAN specification) for nomadic support.
- Longer term interworking based on Mobile IP (MIP) or by optimized and network assisted SIP signalling, for mobility with session continuity support is proposed. The latter targets SIP-based applications and provides continuous (seamless) mobility and privacy protection whereas the former is applicable also to non-SIP-based applications.

Authentication, Authorization and IP addressing

- Authentication in nomadic situations is based on EAP with a decorated NAI to indicate the visited network. Based on the NAI, the EAP messages are routed to the correct AAA server.
- After successful authentication, the terminal receives an IP address from the visited network through DHCP.

Mobile IP

- A Mobility Controller in the Network Service provider to assist in making handover decisions taking into account the resource availability in the access.
- Preference for DS-MIPv6 and PMIPv6 over the other existing MIP flavours, because of their intrinsically good fit in the migration from IPv4 to IPv6 and (in case of DS-MIPv6) the scope for tighter integration with the IP layer for route optimization.

SIP-based mobility

- The SIP-based mobility management solution developed in MUSE achieves adequate mobility management in heterogeneous, multi-provider FMC networks. It is based on two concepts: (1) The IP Soft Handover – P-CSCF (SIP Back-to-Back user agent) and C-BGF functions including RTP proxy and Conferencing module to allow make-before-break seamless handover controlled by the SIP layer and (2) SBC Daisy Chaining – when session/terminal moves from one network served by one SBC to another network served by different SBC, IP Soft Handover capable SBCs are daisy chained to provide seamless handover during such move.

Roaming

- Three types of roaming agreements are sufficient for FMC in an unbundled business environment. This is more than the single roaming agreement in current mobile roaming, but still manageable.

The main points of these architectural recommendations, their relation with 3GPP, ETSI and IETF standards and the main choices made in their protocol implementation have been presented in this white paper. A dedicated MUSE deliverable [7] provides the full architecture including additional, more detailed implementation choices. It also defines the location of the functions that support the described FMC capabilities in the overall GSB architecture.