Ultra Flat Architecture for high bitrate services in fixed mobile convergent networks

D3 Ultra Flat Architecture integration scenarios and their performance analysis and comparison

Editor: Philippe Herbelin, Orange Labs

Suggested readers
Network architects, researchers, service developers

Abstract

With the explosive proliferation of mobile communications and wireless computing devices, the scalability property is becoming an increasingly important feature of wireless communication in pervasive networking scenarios. The Ultra Flat Architecture is a new concept of fixed mobile convergent networks that aims to scale well with the mobile Internet traffic explosion forecasted for the next 5–10 years.

This study presents two integrated protocol scenarios in order to improve handover of SIP and non SIP applications which are:

• 802.21 in combination with HIP and SIP,
• 802.21 in combination with PMIP and SIP.

Both integrated scenarios use the 802.21 MIH framework in combination with MIP or HIP and with SIP. The study will describe:

• The terminal attachment procedures, including AAA, security and IP addressing,
• The session establishment, maintenance and QoS procedures,
• The mobility procedures, including handover initiation, preparation decision, execution and completion phases.

Finally, the performance of the two integrated UFA scenarios will be analysed and compared.

The presented concept of a flat architecture for mobile and convergent networks can form the basis of new research in the future, and can lead to the preparation of a large scale European collaborative project.
Eurescom participants in study P1857 are:
France Telecom - Orange Labs,
Portugal Telecom Inovação,
Mobile Innovation Centre Hungary (MIK).

Ultra Flat Architecture integration scenarios and their performance analysis and comparison
Editor: Philippe Herbelin, France Telecom
Study supervisor: Ádám Kapovits, Eurescom
Eurescom published study result: EDIN 0586-1857
© 2010 Eurescom participants in study P1857

Disclaimer
This report contains material which is the copyright of Eurescom Study Programme Subscribers and may not be reproduced or copied without permission. The information contained in this report is the proprietary confidential information of certain Eurescom Study Programme Participants and may not be disclosed except in accordance with Section 5 of Eurescom’s general conditions of contract.
All Participants have agreed to full publication of the report.
Neither the Participants nor Eurescom warrant that the information contained in the report is capable of use, or that use of the information is free from risk, and accept no liability for loss or damage suffered by any person using the information.
Preface

For mobile operators and networks the challenge in the coming years will be to offer high bitrate data services to mobile customers. At the same time future mobile architectures are being standardized to offer mobility between heterogeneous access technologies. These architectures are primarily centralized that can lead to scalability issues. The study proposes to provide a new architecture that integrates scalability requirements with the reduction of the number of network nodes to one node which is the base station, by the distribution of traditional user and control plane functions in this node. This new ultra flat architecture must optimize service establishment and mobility procedures in a fixed mobile convergence environment.

The main objective of this study is to exchange views between operators concerning 3GPP architectures' limitations and to evaluate the interest in an ultra flat architecture.

More specifically

- Evaluate the limitations regarding scalability, and also from time to market point of view of 3GPP (and 3GPP2) architectures using anchor based mobility;
- Define an ultra flat architecture;
- Assess the advantages (e.g. cost efficiency) of adopting an ultra flat architecture;
- Provide a list of requirements for such an ultra flat architecture.

P1857 started in December 2008 with the participation of France Telecom Orange Labs, Portugal Telecom Inovação and the Mobile Innovation Centre of Hungary (contracted on recommendation and on behalf of Magyar Telekom). The Study is lead by Mr Philippe Herbelin from France Telecom Orange Labs. The study was originally planned to complete in September 2009, but was later extended to allow the performance analysis and comparison of selected integration scenarios.

This is the last Deliverable of the study, titled “Ultra Flat Architecture integration scenarios and their performance analysis and comparison”. The study already produced two deliverables, D1 with the title “Ultra Flat Architecture for high bitrate services in fixed mobile convergent networks”, and D2 with the same title but taking the shape of a set of presentation slides. D2 will be updated with the results contained in this deliverable.
Executive Summary

Why you should read this study report

With the explosive proliferation of mobile communications and wireless computing devices, the scalability property is becoming an increasingly important feature of wireless communication in pervasive networking scenarios, because of its impact on user’s quality of experience. At the same time operators wish to improve the control over their networks with regard to resources and mobility with the proliferation of real time, high bitrate, data intensive mobile access services.

Eurescom study P1857 has designed and proposed a disruptive architecture named Ultra Flat Architecture (UFA) that overcomes the scalability issues by optimizing service establishment and mobility management. The proposed architecture (UFA) gathers session and network resources information in the same equipment, called UFA Gateway (UFA_GW). Through the UFA_GW it becomes possible to simultaneously establish sessions, check network resource availability, manage mobility and adapt the service within the same procedure. UFA permits the removal of centralized elements (like IP anchors) resulting in more efficient procedures and reduced delay. With the distribution of UFA_GWs close to customers scalability can be ensured.

Based on UFA, a flat and fully distributed architecture, two integrated protocol scenarios have been defined:
- 802.21 in combination with HIP and SIP,
- 802.21 in combination with PMIP and SIP.

The benefits for your company

The Ultra Flat Architecture promises to provide the telecom operators with the foundation of a new convergent architecture to anticipate the explosive proliferation of mobile communications and wireless computing devices and real time, high bitrate data services.

Aspects addressed by this study report

The Ultra Flat Architecture is a new concept of fixed mobile convergent networks that aims to scale well with the mobile Internet traffic explosion forecasted for the next 5–10 years. The basic UFA principles were described earlier in [9].

Three main mobility execution algorithms have been analyzed within P1857 that have the potential to be integrated with the 802.21 framework within the UFA:
1) SIP-based,
2) HIP-based,
3) MIP based protocols.

These mobility protocols handle handovers at the application layer, between the application and network layers, and at the network layer, respectively.

P1857 concluded that two integration scenarios based on its findings are worth for further, deeper investigation. This report presents in detail the two integrated protocol scenarios that aim to improve handover of SIP and non SIP applications, which are:
- 802.21 in combination with HIP and SIP,
- 802.21 in combination with PMIP and SIP.

Both integrated scenarios use the 802.21 MIH framework in combination with MIP or HIP and with SIP. The report describes:
- The terminal attachment procedures, including AAA, security and IP addressing,
- The session establishment, maintenance and QoS procedures,
- The mobility procedures, including handover initiation, preparation decision, execution and completion phases.

Finally, the performance of the two integrated UFA scenarios are analysed and compared.
Main findings
The study will provide a description of the Ultra Flat Architecture for the implementation of the two integrated protocol scenarios:

- Description of UFA nodes (UFA_GW, UFA Core Node),
- Description of the functional modules in the UFA_GW,
- Macro definition of the two integrated scenarios,
- The terminal attachment procedures, including AAA, security and IP addressing,
- The session establishment, maintenance and QoS procedures,
- The mobility procedures, including:
  - Media independent handover by using 802.21 framework,
  - End-to-end mobility solutions (i.e., SIP, new delegation-based HIP), and a hierarchical mobility solution (i.e., PMIP),
  - Context transfer between source base station and target base station based on Context Transfer Protocol (CXT).

The comparison of the integrated protocol scenarios has been made according to the kind of applications, SIP applications and non-SIP applications, launched by the mobile nodes to core nodes like servers or equally to other mobile nodes.

We divided the comparison into three main use cases:

1) For non-SIP applications, comparison of the HIP and the PMIP procedures based on UFA signalling schemes,

2) For SIP-applications, we consider and evaluate when mobility execution for SIP applications and non-SIP applications are managed by HIP or PMIP makes the handover (in the same way as for 1), furthermore after physical handover SIP may update the session description protocol (QoS) of the SIP session. SIP re-INVITE procedures have to be added after handover completion of HIP or PMIP, in order to update the session description protocol according to the resources on the T_UFA_GW / candidate L2 point of access.

3) For SIP applications, we consider and evaluate slightly different handover procedures from usecase 2). Now the SIP re-INVITE procedure might replace 802.21 MIH_Net_HO_commit exchange to the mobile node in order to detach from the S_UFA_GW and attach to the T_UFA_GW. Session description protocol update may be performed before the physical handover thanks to the SIP mobility (re-INVITE) procedure. Otherwise, the HIP and PMIP procedures remain the same.

The results show that HIP and PMIP scenarios could introduce too much service interruption delay for real-time SIP applications in usecase 2), hence SIP sessions must update their session description protocol information proactively before physical handover, as it is performed in use case 3).

Under the previously mentioned constraints and simplifications, the HIP based alternative seems to behave slightly better than the PMIP based alternative. However, this is due to the better Denial of Service resistance built-in into HIP, protecting UFA_GWs, and the highly integrated mobility and security control functionalities in the combined HIP based signalling scheme. Note that the proposed HIP module still needs detailed design, development and testing to realize the HIP delegation service functionalities.

Conclusion
In summary, the Eurescom P1857 study has proved that a flat and fully distributed architecture with customized protocols scenarios could provide a solution to the scalability issue of mobile and convergent networks. We believe in the potential of the presented concept of a flat architecture for mobile and convergent networks, and we expect that it will be subject of new research in the future. For example the results of the study will be used as background for the CELTIC project MEVICO, and the partners have plans to submit a new collaborative project proposal to the EC FP7.
List of Authors

Khadija Daoud Triki (FT Orange Labs)
László Bokor (MIK)
Pedro Neves (PT)
Philippe Herbelin (FT Orange Labs)
Ricardo Azevedo (PT)
Zoltán Faigl (MIK)
Table of Contents

Preface ............................................................................................................................................ 3
Executive Summary .......................................................................................................................... 4
List of Authors .............................................................................................................................. 6
Table of Contents .......................................................................................................................... 7
List of Figures ..................................................................................................................................... 9
List of Tables ...................................................................................................................................... 11
Abbreviations .................................................................................................................................... 12

1 Introduction ..................................................................................................................................... 15
   1.1 Context ..................................................................................................................................... 15
   1.2 Objective and scope of this document ...................................................................................... 16
   1.3 Structure of this document ...................................................................................................... 16

2 Description of integration scenarios ............................................................................................ 17
   2.1 802.21 in combination with HIP and SIP ............................................................................... 18
   2.2 802.21 in combination with PMIP and SIP .............................................................................. 19
   2.3 UFA Cross Layer module ....................................................................................................... 20

3 Service establishment and mobility use cases ............................................................................... 21
   3.1 Use-case 1: multi-applications over single interface ................................................................. 21
   3.2 Use case 2: multi-applications over multi interface ................................................................. 22

4 Ultra Flat Architecture integration scenario no.1: 802.21 in combination with HIP and SIP .......... 24
   4.1 Motivations ............................................................................................................................ 24
   4.2 Generic 802.21-HIP-UFA integration scheme ........................................................................ 24
      4.2.1 Architecture description .................................................................................................... 24
      4.2.2 Delegation framework and context transfer ........................................................................ 27
   4.3 Attachment procedure ............................................................................................................ 30
      4.3.1 L2 and HIP access authorization ....................................................................................... 30
      4.3.2 L3 attachment procedure .................................................................................................. 31
   4.4 Session establishment and maintenance .................................................................................. 33
      4.4.1 Non-SIP applications establishment ................................................................................... 33
      4.4.2 SIP applications establishment ........................................................................................ 34
   4.5 Mobility procedures ................................................................................................................. 35
      4.5.1 Handover initiation ............................................................................................................ 35
      4.5.2 Handover preparation phase .............................................................................................. 36
      4.5.3 Handover execution phase ................................................................................................ 40
      4.5.4 Handover completion phase ............................................................................................. 42

5 Ultra Flat Architecture integration scenario no.2: 802.21 in combination with PMIP and SIP ....... 44
   5.1 Proxy MIP and UFA Integration Overview .............................................................................. 44
   5.2 Attachment procedure ............................................................................................................. 45
      5.2.1 Registration / Authentication procedure ............................................................................ 45
      5.2.2 PMIP initialisation procedure ............................................................................................. 46
   5.3 Session establishment and maintenance .................................................................................... 48
      5.3.1 SIP applications ................................................................................................................ 48
      5.3.2 Non-SIP applications ........................................................................................................ 50
5.4 Mobility procedures .................................................................................................................. 50
  5.4.1 Handover initiation phase ................................................................................................. 50
  5.4.2 Handover preparation ...................................................................................................... 51
  5.4.3 Handover decision phase ............................................................................................... 53
  5.4.4 Handover execution phase mobile-initiated ................................................................. 54
  5.4.5 Handover execution phase network-initiated ............................................................... 56
  5.4.6 Handover completion phase ......................................................................................... 57

6 UFA integration scenario analysis ................................................................................................. 59
  6.1 Objectives for the evaluation ............................................................................................. 59
  6.2 Decision criteria .................................................................................................................. 60
  6.3 Network model for performance evaluation ....................................................................... 62
  6.4 Features of the alternatives influencing the evaluation under different criteria ................. 63
  6.5 Evaluation results ............................................................................................................... 66
    6.5.1 Terminal scores of the alternatives under the defined criteria set and weights .......... 66
    6.5.2 Sensitivity of the terminal scores to the network delay between the MN and the UFA_GW69
    6.5.3 Sensitivity of the terminal scores to the weights of the main criteria ...................... 73
  6.6 Discussion of the results ...................................................................................................... 77

7 Conclusion ..................................................................................................................................... 78

Annex A Registration/authentication procedures defined in 3GPP standards ................................ 80
Annex B EAP-AKA authentication defined in 3GPP standards for non-3GPP access networks... 84
Annex C IP address allocation in 3GPP standards for non-3GPP access networks ...................... 88
Annex D IPsec Tunnel context ....................................................................................................... 90
Annex E L2 fast re-authentication techniques ............................................................................. 91
    E.1 Access technology dependent L2 fast re-authentication techniques ......................... 91
    E.2 EAP and ERP for L2 handovers .................................................................................... 91
    E.3 Inter-AAA L2 handovers ............................................................................................ 91
Annex F Criterion weight specification forms ............................................................................ 92
Annex G Analysis of the message traces of the procedures ...................................................... 96
Annex H References ..................................................................................................................... 105
List of Figures

Figure 1: Ultra Flat Architecture ........................................................................................................... 17
Figure 2: UFA_GW modules interaction in HIP scenario ........................................................................ 18
Figure 3: UFA_MW or UFA_CN modules interaction in HIP scenario ................................................... 18
Figure 4: UFA_GW modules interaction in PMIP-SIP scenario ............................................................... 19
Figure 5: UFA_MW or UFA_CN modules interaction in MIP scenario .................................................. 19
Figure 6: Mobility usecase 1 .................................................................................................................. 21
Figure 7: Mobility usecase 2 .................................................................................................................. 22
Figure 8: HIP-based Ultra Flat Architecture .......................................................................................... 25
Figure 9: Traffic forwarding in HIP-based UFA architecture using IPsec “tunnels” ................................. 26
Figure 10: SPI-based traffic forwarding ................................................................................................. 26
Figure 11: Registration to Type 1/2 Delegation Service and requesting Type 1 .................................... 27
Figure 12: Requesting Type 2 Delegation Service ................................................................................ 29
Figure 13: Public key authorization certificates defined for delegation ................................................. 29
Figure 14: L2 attachment procedure ....................................................................................................... 31
Figure 15: Bootstrapping the MN, and HIP-level attachment procedure ............................................. 32
Figure 16: L3 attachment procedure ..................................................................................................... 33
Figure 17: Session establishment and maintenance procedures in the 802.21-HIP-SIP UFA integration scenario ........................................................................................................................................... 33
Figure 18: SIP Session establishment procedure in the 802.21-HIP-SIP scenario, part I ....................... 34
Figure 19: SIP Session establishment procedure in the 802.21-HIP-SIP scenario, part II ...................... 35
Figure 20: Handover initiation ................................................................................................................ 35
Figure 21: Handover preparation ............................................................................................................ 37
Figure 22: HIP Handover preparation (Part 1) ....................................................................................... 39
Figure 23: HIP handover preparation (Part 2) ....................................................................................... 40
Figure 24: L2 handover execution .......................................................................................................... 41
Figure 25: SIP handover execution for HIP scenario option 3 .............................................................. 42
Figure 26: Handover completion phase .................................................................................................. 43
Figure 27: UFA and PMIP Architecture ................................................................................................. 44
Figure 28: Registration / Authentication procedure .............................................................................. 46
Figure 29: PMIP initialisation procedure ............................................................................................... 47
Figure 30: Service establishment call-flow – SDP Offer/Answer ........................................................... 48
Figure 31: Service establishment call-flow – SDP Confirmation ............................................................ 50
Figure 32: Handover Initiation Phase ..................................................................................................... 51
Figure 33: Handover Preparation Phase – Centralized procedure .......................................................... 52
Figure 34: Handover Preparation Phase- Distributed procedure ............................................................. 53
Figure 35: Handover Decision Phase ..................................................................................................... 54
Figure 36: Handover Execution Phase mobile-initiated .......................................................................... 55
Figure 37: Handover Execution Phase network-initiated – Option 1 ...................................................... 56
Figure 38: Handover Execution Phase network-initiated – Option 3 ...................................................... 57
Figure 39: Handover Completion Phase .................................................................................................. 57
Figure 40: Handover completion phase – SIP registration .................................................................... 58
Figure 41: Criterion tree. ....................................................................................................................... 60
Figure 42: Geometric scale types ................................................................. 62
Figure 43: UFA network model ................................................................. 62
Figure 44: Terminal scores of the alternatives in the two network scenarios ......................................................... 67
Figure 45: Terminal scores of the alternatives under the two network scenarios, with smoother pre-assumptions ........................................................................................................ 68
Figure 46: Sensitivity of the ranking of alternatives to the one-way delay between the MNs and their serving UFA_GWs (CNs are also MNs). ........................................................................................................... 71
Figure 47: Sensitivity of the ranking of alternatives to the average one-way delay between the MN and the UFA_GWs (CNs are servers). ........................................................................................................... 73
Figure 48: Terminal scores of the alternatives under perturbed criteria weights, in function of the performance criterion weight ........................................................................................................... 74
Figure 49: Terminal scores of the alternatives under perturbed criteria weights, in function of the security criterion weight ........................................................................................................... 75
Figure 50: Terminal scores of the alternatives under perturbed criteria weights, in function of the deployment criterion weight ........................................................................................................... 76
Figure 51. Registration / Authentication procedure to access network and IMS as defined in the standard ........................................................................................................................................ 80
Figure 52. ATH_5. Registration/authentication to IMS ........................................................................................................... 82
Figure 53. EAP-AKA authentication procedure ........................................................................................................... 84
List of Tables

Table 1. Explanation of HIP-based delegation service messages ................................................. 28
Table 2: Parameters used in our network model. .............................................................................. 63
Table 3: Surplus protocol modules for the alternatives beyond the TCP/IP stack ......................... 63
Table 4: Security features of the HIP and PMIP based signalling schemes ................................ 63
Table 5: The signalling demands on different network parts given in number of messages from different aspects for the evaluation of the performance cost sub-criteria ........................................ 65
## Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>3GPP</td>
<td>Third Generation Partnership Project</td>
</tr>
<tr>
<td>AAA</td>
<td>Access, Authorization, and Accounting</td>
</tr>
<tr>
<td>AKA</td>
<td>Authentication and Key Agreement</td>
</tr>
<tr>
<td>AN</td>
<td>Access Node</td>
</tr>
<tr>
<td>AS</td>
<td>Application Server</td>
</tr>
<tr>
<td>AUTN</td>
<td>Authentication Token</td>
</tr>
<tr>
<td>B2BUA</td>
<td>Back-to-Back User Agent</td>
</tr>
<tr>
<td>BEET</td>
<td>A Bound End-to-End Tunnel</td>
</tr>
<tr>
<td>BEX</td>
<td>(HIP) Base Exchange</td>
</tr>
<tr>
<td>CK</td>
<td>Cipher Key</td>
</tr>
<tr>
<td>CN</td>
<td>Correspondent Node</td>
</tr>
<tr>
<td>CPH</td>
<td>Control Plane Header</td>
</tr>
<tr>
<td>CSCF</td>
<td>Call Service Control Function</td>
</tr>
<tr>
<td>CXTP</td>
<td>Context Transfer Protocol</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DSRK</td>
<td>Domain Specific Root Key</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>EMSK</td>
<td>Extended Master Session Key</td>
</tr>
<tr>
<td>EPC</td>
<td>Evolved Packed Core</td>
</tr>
<tr>
<td>EPS</td>
<td>Evolved Packet System</td>
</tr>
<tr>
<td>ERP</td>
<td>EAP Re-authentication Protocol</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulating Security Payload</td>
</tr>
<tr>
<td>E-UTRAN</td>
<td>Evolved UTRAN</td>
</tr>
<tr>
<td>FQDN</td>
<td>Fully Qualified Domain Name</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>HA</td>
<td>Home Agent</td>
</tr>
<tr>
<td>hIK</td>
<td>HIP Integrity Key</td>
</tr>
<tr>
<td>HIP</td>
<td>Host Identity Protocol</td>
</tr>
<tr>
<td>HI</td>
<td>Host Identifier</td>
</tr>
<tr>
<td>HIT</td>
<td>Host Identity Tag</td>
</tr>
<tr>
<td>HLR</td>
<td>Home Location Register</td>
</tr>
<tr>
<td>HLR</td>
<td>Home Location Register</td>
</tr>
<tr>
<td>HMAC</td>
<td>Hashed Message Authentication Code</td>
</tr>
<tr>
<td>HPLMN</td>
<td>Home PLMN</td>
</tr>
<tr>
<td>HoA</td>
<td>Home Address</td>
</tr>
<tr>
<td>HO</td>
<td>HandOver</td>
</tr>
<tr>
<td>HSS</td>
<td>Home Subscriber Server</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>I-CSCF</td>
<td>Interrogating-CSCF</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IK</td>
<td>Integrity Key</td>
</tr>
<tr>
<td>IMPI</td>
<td>IP Multimedia Private Identity</td>
</tr>
</tbody>
</table>
IMPU  IP Multimedia Public Identity  
IMS   IP Multimedia Subsystem  
IMSI  International Mobile Subscriber Identity  
IP    Internet Protocol  
IPSEC IP Security  
IS    Information System  
ITU   International Telecommunications Union  
LLC   Link Layer Control  
LMA   Local Mobility Anchor  
LTE   Long Term Evolution  
MAC   Medium Access Control  
MAG   Mobile Access Gateway  
MB    MiddleBoxe  
MIH   Media Independent Handover  
MIIS  Media Independent Information Service  
MIP   Mobile IP  
MN    Mobile Node  
MPLS Multi Protocol Label Switching  
P-CSCF Proxy-CSCF  
PD    Prefix Delegation  
PDG   Packet Data Gateway  
PLMN  Public Land Mobile Network  
PMIP  Proxy MIP  
PoA   Point of Access  
PoS   Point of Selection  
QoS   Quality of Service  
RAND  Random Number  
RTP   Real time Transport Protocol  
RVS   Rendez-Vous Server  
SA    Security Association  
SAP   Service Access Point  
S-CSCF Serving-CSCF  
SDP   Session Description Protocol  
SGSN  Serving GPRS Support Node  
S-GW  Serving Gateway  
SIM   Subscriber Identity Module  
SIP   Session Initiation Protocol  
SPD   Security Policy Database  
SPI   Security Parameter Index  
TCP   Transmission Control Protocol  
UA    User Agent  
U-CSCF UFA-CSCF  
UE    User Equipment / User Entity  
UFA   Ultra Flat Architecture
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UFA_CL</td>
<td>UFA_Cross Layer</td>
</tr>
<tr>
<td>UFA_GW</td>
<td>UFA_GateWay</td>
</tr>
<tr>
<td>UMTS</td>
<td>UMTS - Universal Mobile Telecommunications System</td>
</tr>
<tr>
<td>UPSF</td>
<td>User Profile Server Function</td>
</tr>
<tr>
<td>URI</td>
<td>Uniform Resource Identifier</td>
</tr>
<tr>
<td>VPLMN</td>
<td>Visited PLMN</td>
</tr>
<tr>
<td>WiFi</td>
<td>Wireless Fidelity</td>
</tr>
<tr>
<td>WiMAX</td>
<td>Worldwide Interoperability for Microwave Access</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>XRES</td>
<td>Expected Response</td>
</tr>
</tbody>
</table>
1 Introduction

1.1 Context

Having identified IEEE 802.21 as a candidate standard for optimizing the mobility management procedures in heterogeneous environments, this task intends to thoroughly investigate candidate integration scenarios between 802.21 and the MIP, HIP and SIP protocols under the UFA paradigm.

IEEE 802.21 describes a framework that supports both mobile node and network side handover decisions, the collection of necessary information from different parts and layers of the network, and it remains open for the mobility execution algorithm. Mobility execution algorithms, such as MIP, HIP and SIP, execute the tasks related to terminal mobility and ongoing sessions. Such functions include location updates at location information services and location updates at correspondent nodes. Handover also implies the need for QoS information updates in existing sessions.

Three main mobility execution algorithms have been analyzed within P1857 that have the potential to be integrated with the 802.21 framework within the UFA: 1) SIP-based, 2) HIP-based and 3) MIP based protocols. They handle handovers at the application layer, between the application and network layers, and at the network layer, respectively.

The study so far has concluded that two integration scenarios based on its findings are worth for further, deeper investigation:

- 802.21 in combination with HIP and SIP,
- 802.21 in combination with PMIP and SIP.

This task will provide a description of the UFA_GW architecture for the implementation of the two integrated scenarios:

- Description of UFA nodes (UFA_GW, UFA Core Node),
- Description of the functional modules in the UFA_GW,
- Macro definition of the two integrated scenarios.

The task will then go on and define the service establishment and mobility use cases that will be used by the two integration scenarios to describe the UFA procedures.

Both integrated scenarios use the 802.21 MIH framework in combination with MIP or HIP and with SIP. They cover:

- The terminal attachment procedures, including AAA, security and IP addressing,
- The session establishment, maintenance and QoS procedures,
- The mobility procedures, including,
  - Media independent handover by using 802.21 framework,
  - End-to-end mobility solutions (i.e., SIP, new delegation-based HIP), and a hierarchical mobility solution (i.e., PMIP).
  - Context transfer between source base station and target base station (e.g. 802.21, SIP, Context Transfer Protocol (CXTP) [17]).

Finally, the performance of the two integrated UFA scenarios will be analysed and compared.
1.2 Objective and scope of this document

The goal of this Eurescom study is to investigate the design of two integrated scenarios over an Ultra Flat Architecture in order to provide a scalable convergent architecture and to optimize attachment, session establishment and mobility procedures.

The document will describe all the procedures for the two integrated scenarios, with the objective to make performance comparison:

- 802.21 in combination with HIP and SIP,
- 802.21 in combination with PMIP and SIP.

1.3 Structure of this document

The reminder of this document is organized as follow:

- Chapter 2: Description of integration scenarios
  - The two integrated scenarios will be introduced and the main modules will be listed.
- Chapter 3: Service establishment and mobility use cases
  - This chapter will define the different use-cases that will be used in chapter 4 and 5 to define the establishment and mobility procedures.
- Chapter 4: Ultra Flat Architecture integration scenario no.1: 802.21 in combination with HIP and SIP
  - This chapter will describe all the procedures of the 802.21 - HIP -SIP scenario 802.21 according to the mobility use cases.
- Chapter 5: Ultra Flat Architecture integration scenario no.2: 802.21 in combination with PMIP and SIP
  - This chapter will describe all the procedures of the 802.21 - PMIP -SIP scenario 802.21 according to the mobility use cases.
- Chapter 6: UFA integration scenario analysis
  - Based on the description of the two integrated scenarios for UFA, this chapter will analyse and compare their performances thanks to the evaluation method named Multiplicative Analytic Hierarchy Process.
- Chapter 7: Conclusion
  - Finally, this chapter will conclude the study of two protocol scenarios for UFA.
- Annex A: Registration/authentication procedures defined in 3GPP standards
- Annex B: EAP-AKA authentication defined in 3GPP standards for non-3GPP access networks
- Annex C: IP address allocation in 3GPP standards for non-3GPP access networks
- Annex D: IPsec Tunnel context
- Annex E: L2 fast re-authentication techniques
- Annex F: Criterion weight specification forms
- Annex G: Analysis of the message traces of the procedures
2 Description of integration scenarios

For an UFA, the study so far have concluded that two integration scenarios based on its findings are worth for further, deeper investigation:

1. 802.21 in combination with HIP and SIP,
2. 802.21 in combination with PMIP and SIP.

According to the kind of applications requested by a MN, a set of modules of the UFA_GW will be in charge of a cross-layer optimization.

Figure 1: Ultra Flat Architecture
2.1 802.21 in combination with HIP and SIP

For this scenario, the interaction between modules is depicted in Figure 2. The main modules of this scenario are:

- 802.21 for establishing the communication between UFA_GW and MNs, and also between UFA_GWs,
- SIP module, named U-CSCF when the UFA_GW is connected to an IMS network,
- HIP module for delegation-based session establishment, mobility procedures, and security control in the UFA,
- UFA Cross-layer module in charge of the intelligence of the UFA_GW to correlate the communication between the different modules and also with other UFA nodes (MN, CN, UFA core nodes and with other UFA_GWs).

![Figure 2: UFA_GW modules interaction in HIP scenario](image)

The UFA_CL module will not be implemented only in the UFA_GW. This module will be also implemented in the UFA_MN and potentially in UFA_CN when the UFA_CN is a server.

![Figure 3: UFA_MW or UFA_CN modules interaction in HIP scenario](image)

All the interaction between these modules will be described in chapter 4, thanks to the definition of all the procedures.
2.2 802.21 in combination with PMIP and SIP

For this scenario, the interaction between modules is depicted in Figure 4. The main modules of this scenario are:

- 802.21 for establishing the communication between UFA_GW and MNs, and also between UFA_GWs,
- SIP module, named U-CSCF when the UFA_GW is connected to an IMS network,
- PMIP module for executing the mobility management procedures at the IP layer
- UFA Cross-layer module in charge of the intelligence of the UFA_GW to coordinate the communication between the different modules and also with other UFA nodes (MN, CN, UFA core nodes and other UFA_GWs.

![Figure 4: UFA_GW modules interaction in PMIP-SIP scenario](image)

The UFA_CL module will not be implemented only in UFA_GW it might be necessary in the UFA_MN and potentially in UFA_CN when the UFA_CN is a server.

![Figure 5: UFA_MW or UFA_CN modules interaction in MIP scenario](image)

All the interaction between these modules will be described in chapter 5, thanks to the definition of all the procedures.
2.3 UFA Cross Layer module

UFA Cross-layer module (UFA_CL) is the intelligence of the UFA_GW to correlate the communication between the different modules and UFA nodes (MN, CN, UFA core nodes and other UFA_GWs).

The UFA_CL is in charge of the control of all the procedures inside the UFA_GW. It manages the MN authentication, ensures the role of the security manager and it is in charge of making handover decisions for the established sessions. It uses the MIH framework for the collection of static and dynamic input data for intelligent decision making, resource reservation in target UFA_GWs and target PoAs. From the MIH aspect it acts as a MIH user. Furthermore, it must take into account the routing and mobility policies for different SIP and non-SIP application types for handover decisions and mobility management.

For the mobility procedure, according to the applications requested by the MN, the UFA_CL module will execute SIP mobility mechanisms for SIP based applications and will execute HIP or PMIP mobility procedures for non-SIP based applications. All the procedures according to applications establishment and mobility use-cases will be defined in chapter 4 and 5 for:

- The terminal attachment procedures, including AAA, security and IP addressing,
- The session establishment, maintenance and QoS procedures,
- The mobility procedures, including,
  - Media independent handover by using 802.21 framework,
  - End-to-end mobility solutions (i.e., SIP, new delegation-based HIP), and a hierarchical mobility solution (i.e., PMIP).
  - Context transfer between source base station and target base station based on Context Transfer Protocol (CXTP) [17].
3 Service establishment and mobility use cases

This chapter defines the different use-cases that will be used in chapter 4 and 5 to define the establishment and mobility procedures.

The main idea is to consider that the UFA_MN will use SIP applications and non-SIP applications. Use cases will propose to consider MN with a single interface or multiple interfaces.

The term "SIP applications" means any kind of application that requires SIP protocol for the session establishment, controlled by the network operator.

The term "non-SIP applications" means any kind of application that does not require SIP protocol for the session establishment. It concerns TCP/IP applications like HTTP. SIP could be used also but it is nor controlled by one network operator.

3.1 Use-case 1: multi-applications over single interface

UFA_MN requests one SIP application and one non-SIP application throughout the Source UFA_GW. It concerns multi-applications (SIP and non-SIP applications) with a single interface for the UFA_MN. A hard-handover will be executed. Usecase 1 seems to be the worst technical usecase to describe.

When a MN established sessions for SIP applications and non SIP applications as described in Figure 6, for this use case, we could consider three different handover processes:

1. Option 1: HIP or PMIP mobility execution for SIP applications and non-SIP applications. How do we handle to adapt QoS for SIP applications during the handover, especially for downgrading the QoS of the SIP application due to lack of resources on the target UFA_GW?
If we consider that SIP applications could be upgraded after the handover, it is not really an issue. It could be controlled by the target UFA_GW.

2. Option 2: SIP mobility execution for SIP applications and HIP or PMIP mobility applications for non-SIP applications → the two different processes should be synchronised. If the two processes are not synchronised, the MN might detach from the Source UFA_GW before two mobility executions are finished.

3. Option 3: The SIP re-INVITE procedure might replace 802.21 MIH_Net_HO_commit exchange to the MN in order to detach from the S_UFA_GW and attach to the T_UFA_GW. SDP update may be performed before the physical handover thanks to the SIP mobility (re-INVITE) procedure. Otherwise, the HIP and PMIP procedures remain the same as in Option 1 and 2.

What will happen if the MN establishes only non-SIP applications? If that case, mobility execution will be based only on HIP or PMIP procedure. A SIP register will be launched to the REGISTRAR after the handover execution to inform the core network form the MN location.

For the scenarios description, option 1 and option 3 have been selected, developed and detailed.

### 3.2 Use case 2: multi-applications over multi interface

This use case concerns multi-applications for multi-interface. A soft-handover could be executed.

![Figure 7: Mobility usecase 2](image)

For this use case mobility procedure should be able to execute the handover of applications in a per-application basis. SIP and HIP mobility procedures could be executed in parallel.
Mobility execution could be based on soft-handover. In soft handover [26] (make-before-break), MN maintains simultaneously multiple air interface connections to different UFA_GWs. When a MN sees several UFA_GWs in the active set, it can attach to a new one before it drops radio link in old UFA_GW. But it should last as short time as possible:

- Zero packet loss
- Short delay for the handover with the two interfaces up to optimize energy
4 Ultra Flat Architecture integration scenario no.1: 802.21 in combination with HIP and SIP

4.1 Motivations

The inseparable bond between the locator and identifier functions of IP makes it inconvenient or even impossible to design efficient and scalable mobility, multihoming, traffic engineering, routing and security solutions in future mobile architectures. Supporting heterogeneous network layer protocols or different locator families is also limited because of the same reason. The general concept of ID/Loc separation aims to eliminate the above problems and limitations by splitting the two roles of IP addresses and such allowing network layer to change locators without interfering with upper layer procedures. The problem also has recently been introduced in the standardization activities of ITU-T for integration in future network architectures [10], [11].

In this chapter we propose a new UFA signalling scheme where we apply the Host Identity Protocol (HIP) that is an instance protocol providing a logical overlay for ID/Loc separation with cryptographic IDs (i.e., Host Identifiers - HIs) generated from a new, statistically globally unique namespace called Host Identity. In this namespace a Host Identifier is the public key of an asymmetric key-pair which is thus self-certifying. HIP includes all the modifications and methods that allow integrating the ID/Loc concept into the existing Internet architecture. These functions form a new protocol layer, which resides between the transport and network layer. For further information about HIP and its extensions see the first deliverable (P1857-D1).

4.2 Generic 802.21-HIP-UFA integration scheme

4.2.1 Architecture description

Our proposal for a HIP-based Ultra Flat Architecture is depicted in Figure 8. The architecture comprises:

1) Several access networks (both wired and wireless),
2) An IP/MPLS transit network,
3) An IEEE 802.21 MIH management subsystem,
4) A HIP-based control network.

To address scalability issues detailed in the first deliverable [9], centralized IP anchors between Point of Access (PoA) nodes and correspondent nodes are removed, and network functions are placed at the edge of the transit and access networks (close to the Point of Access (PoA) nodes) in the Ultra Flat Architecture Gateways (UFA GWs). UFA GWs control the procedures described in the following Sections.

Heterogeneous access networks provide the air interface for mobiles making them able to connect to the core infrastructure (and to the Internet) anytime, anywhere. Besides to support IEEE 802.21 mechanisms there are no other restrictions regarding the access technologies to be used in this framework: any kind of access system can be applied in any kind of heterogeneous setup.

The IP/MPLS transit network is the operator’s backbone including routers and core network elements (for service and configuration provision, 802.21 services etc.), and natively connecting UFA to the global backbone (i.e., to the Internet). Locators used in the transit network are global locators while locators in the access networks are local locators.
The IEEE 802.21 MIH management subsystem will handle handover preparation issues and relating signalling tasks in order to initiate HIP handover procedures in UFA and to support network and mobile controlled handover decision. This subsystem relies on the existing methods, messages and primitives of the 802.21 standard. In this scheme, network initiated 802.21 handover preparation procedures are triggered by UFA GWs (refer to Appendix C.2 in [13]), and RP3/RP5 messages are sent over L3 [14], and protected by HIP and IPsec.

The control network in the upper part of Figure 8 contains a HIP-compatible Domain Name System [12] for resolving domain names to host identities and/or locators depending on the actual situation. In addition there is the HIP Control Plane which stores and distributes dynamic and presumably frequently changing binding information between host identities and locators of all actively communicating (mobile) hosts in UFA. This control plane might be a conventional RVS [15] park or a complete distributed HIP signalling architecture like Hi3 [16]. The records managed here are provided by the UFA_GWs using their own global locators as location information to be bounded with identities of their actively interacting partners.

Based on the cooperation of the above main architectural elements our proposed framework transports end-to-end flows between MNs and CNs in a hop-by-hop manner. Here every packet holds HIT information (similarly to Control Plane Header (CPH) proposed in [18]) and HIT-based mapping is to be introduced in UFA_GWs – as middle hops – for the hop-by-hop packet transfer. Figure 9 illustrates traffic forwarding in HIP-based UFA.
SPI collisions can be avoided during HIP BEX

<table>
<thead>
<tr>
<th>L2 header</th>
<th>IP header</th>
<th>ESP header</th>
<th>Control Plane header</th>
<th>Payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>CPH = src HIT, dst HIT, [higher layer selectors]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Hop-by-hop paradigm „tunnel“ mode IPsec: i.e., the inner header is the Control Plane Header or an IP header

Figure 9: Traffic forwarding in HIP-based UFA architecture using IPsec “tunnels”.

UFA GWs are also the delegates of the end peers performing optimization in resource utilization. Hence the main tasks of UFA GWs in this proposal:

1. Helping L2 attachment procedures
2. Controlling mutual authentication
3. Actively interacting with hosts through HIP BEX and signalling delegation for IPsec tunnel management and context transfers
4. Performing the actual mapping/routing between outer header IPsec tunnels based on inner header identifiers
5. Controlling 802.21 mechanisms

Note, that a SPINAT-based [18] HIP UFA signalling architecture was also considered, but finally not chosen. It assumes that end-to-end IPsec SAs are used between the MNs and the CNs. Traffic is forwarded based on the SPI values and destination address of the IP datagram, depicted in Figure 10. In this case SPI collision must be handled for new sessions, in order to provide obvious routing rules in the middleboxes. This can be handled by SPI translation [18], a technique similar to NAT. Stripped End-to-End Tunnel (SEET) mode IPsec is a Bound End-to-End Tunnel (BEET) (or other) mode IPsec ESP, but it is special for not covering the SPI value in the ESP header with integrity protection. It is used in middleboxes (MBs) applying SPI translations on end-to-end IPsec ESP traffic flows

Figure 10: SPI-based traffic forwarding.
4.2.2 Delegation framework and context transfer

In general, delegation of signalling rights is motivated by the optimization of resource utilization between the delegator and the delegate. Delegates are temporarily authorized by the delegator to proceed in certain tasks, such as periodic location updates, rekeyings. The delegator may issue a public-key authorization certificate [19] to the delegate to proceed in his name at the peers. HMAC key can also be issued to a delegate in order to generate HMACs admitted by the peer [20]. Before right delegation it is important that the delegator establishes trust relationship with the delegate, i.e., the identity of the delegate must be authenticated. Delegation chains require implicit trust chains.

In our framework two novel HIP based delegation service types – the bedrocks of our HIP-based UFA signalling scheme – are introduced. On one hand they will help us to reduce the number of DH key exchanges and puzzle solutions in user equipments by decreasing number of HIP BEXs between communicating end terminals. On the other hand delegate UFA_GWvs remove overhead from wireless links by shifting significant part of signalling overhead of MNs from the air interface to the wired UFA segment. Both of the defined HIP delegation service types require preliminary registration procedure called Delegation Establishment as depicted in the upper part of Figure 11. An existing HIP and IPsec association (i.e. completed BEX) is presumed between the Delegator and the Delegate or must be created upon the Delegation Establishment. Also both services rely on the messages and parameters drafted in Table 1.

![Figure 11: Registration to Type 1/2 Delegation Service and requesting Type 1 Delegation Service](image)

In case of Type 1 Delegation (on the bottom of Figure 11) states are established through the Delegate but maintained directly by the Delegator after context transfer. Here, the Delegator asks the Delegate to establish HIP and IPsec states between Delegator and specified nodes (CNs), and then transfer established states from Delegate to Delegator. The existing IPsec and HIP associations between the Delegate and the CN must not be deleted or moved: it provides a base for creating the new IPsec and HIP associations between the Delegator and the CN. It is important that SPI collision is to be avoided at the Delegator and the CNs, not at the Delegate (that is why the Delegator sends its favorable SPI range). The created states are transferred to the Delegator using CTXP messages [17] over the presumed IPsec SAs.
In our HIP-based UFA scheme, this delegation type is employed during handover execution when T UFA GW will ask S UFA GW to create states between itself and the MN and MN’s peer nodes.

Table 1. Explanation of HIP-based delegation service messages

<table>
<thead>
<tr>
<th>HIP Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delegation Establishment Request</td>
<td>The Delegator sends to the Delegate for itself or on behalf of another node in order to request Type 1 / 2 delegation service using HIP REG REQ parameter. Authorization Certificate chain of the acquiring node must be included in HIP NOTIFICATION parameter(s).</td>
</tr>
<tr>
<td>Delegation Establishment Response</td>
<td>The Delegate sends to the Delegator in order to acknowledge or reject Type 1/2 delegation service establishment using HIP REG RESP or REG FAILED parameter.</td>
</tr>
<tr>
<td>Delegation Action Request</td>
<td>The Delegator sends to the Delegate for itself or on behalf of another node in order to request HIP and/or IPsec association creation or update. In case of Type 1 Delegation Service the state information will be transferred to the Delegator. For Type 2 Delegation Service, the states resulted by the action will be created and further maintained by the Delegate.</td>
</tr>
<tr>
<td>Delegation Action Response</td>
<td>The Delegate sends to the Delegator in order to report the Type 1/2 delegation action results in HIP NOTIFICATION parameter(s).</td>
</tr>
<tr>
<td>Mandated Action Request</td>
<td>The Delegator sends to 3rd party node(s). For Type 1 Delegation Service HIP and/or IPsec associations will be created by the Delegate and transferred to the Delegator. In case of Type 2 Delegation Service, new HIP and/or IPsec states are created on behalf of the Delegator by the Delegate and/or traffic mapping rules will be updated. HIP NOTIFICATION parameters are used to transfer the required information such as supported IPsec SPI values of the Delegator, global locator(s) of the Delegator, list of supported HIP and IPsec transforms, traffic mapping rules, Delegator peer list, configuration and service registration parameters, etc.</td>
</tr>
<tr>
<td>Mandated Action Response</td>
<td>3rd party node(s) send to the Delegate in order to report Type 1/2 mandated action results in HIP NOTIFICATION parameter(s).</td>
</tr>
<tr>
<td>Context Transfer Data (CTD)</td>
<td>Sent by the Delegate to Delegator, and includes feature data (i.e., HIP and IPsec context data).</td>
</tr>
<tr>
<td>Context Transfer Data Reply (CTDR)</td>
<td>Sent by Delegator to Delegate, indicating success or failure of context transfer.</td>
</tr>
</tbody>
</table>

In case of Type 2 Delegation (Figure 12) the Delegator requires the Delegate to establish HIP and IPsec states for itself at specified peer nodes and also asks the Delegate to further maintain the created local states. During this type of delegation, SPI collision is to be avoided at the Delegate and the CNs side (not at the Delegator), however it is handled by basic HIP mechanisms. In HIP-based UFA, this delegation type is applied for HIP and IPsec association establishment between the MN and a CN or the MN and an RVS. Here the UFA_GW is the Delegate of the MN in order to maintain HIP and IPsec states on behalf of its Delegator. During handover execution, location update at CNs for MN is initiated by the T_UFA_GW: in that case the T_UFA_GW acts as a Type 2 Delegate of the MN and the S_UFA_GW. Here we capitalize the feature that Type 2 Delegation service enables indirect authorizations, i.e., the use of certificate-chains. E.g., if a T_UFA_GW does not have the authorization certificate of MN, it may still have an authorization from the S_UFA_GW, while the S_UFA_GW has the MN’s authorization.
In our signalling scheme, we apply public key authorization certificates for both type of delegation containing the following information:

\[
\{K_{\text{delegator}}, K_{\text{delegate}}, \text{roles}, \text{restrictions}\} \text{ }_{K_{\text{delegator}}}
\]

Figure 12: Requesting Type 2 Delegation Service

Figure 13: Public key authorization certificates defined for delegation
4.3 Attachment procedure

4.3.1 L2 and HIP access authorization

In UFA one design issue is to avoid duplicate authentication procedures with remote AAA servers on L2 and HIP level. In operator-based environments, the network access authentication on L2 involves the AAA server (and HSS) in the core network.

We suppose that L2 access authorization builds upon an EAP authentication method, such as the EAP-AKA or EAP-SIM [23]. See Annex B for the description of the steps of the EAP-AKA L2 authentication. We also suppose that EAP Re-authentication Protocol (ERP) [21] is deployed using local or home EAP re-authentication (ER) servers to provide fast L2 re-authentications when the MN moves to a new EAP authenticator.

Figure 14, and later Figure 15, illustrate the access authorization concept for the UFA. In these figures, the UFA_GW contains the EAP authenticator, the home AAA server includes the EAP server and the EAP re-authentication server. The UFA_GW or an AAA proxy near the UFA_GW may include the local ER server. The figures illustrate the prerequisites and the functioning of our proposed HIP-level access authorization.

Our proposal requires the introduction of new HIP notification parameters, and two EAP message types, as shown in the final message exchange between the MN and the local ER server in Figure 15. Moreover, we define a new key hierarchy to generate cryptographically separate keys from the session keys provided by ERP and EAP L2 authentications.

The Extended Master Session Key (EMSK) is created after a successful EAP authentication, assuming that it is supported by the chosen L2 EAP authentication method. The EMSK can be used to create usage specific root keys (RK) for any purpose. We propose to create a new usage specific root key for HIP-level fast access authorization, according to [27]. A HIP access authorization root key (hRK) is derived from the EMSK or from the Domain Specific Root Key (DSRK) in home and local ER servers, respectively. The difference between local and home ER servers is that local ER servers are located near the UFA_GW, and derive domain specific HIP peer authorization root keys (DS-hRK) from DSRK, while home ER servers derive HIP peer authorization root keys (hRK) from the EMSK. The DSRK is derived by the home ER server based on the local ER domain name and the EMSK. DSRK is transferred from the home server to the local ER server in the EAP-Success message. AAA protocols, such as Radius or DIAMETER, support EAP transport between the authenticator and the local and home ER servers. Between the MN and the authenticator the EAP transport is L2-specific.

From the HIP root key (hRK or DS-hRK, referred to as hRK in the followings), a HIP integrity key (hIK) is derived. This is used to mutually authenticate, i.e., prove the possession of hRK, between the MN and the local ER server during HIP BEX.
4.3.2 L3 attachment procedure

After successful L2 authentication the MN must acquire bootstrapping parameters, i.e., it must acquire local or remote IP address, or other local or global locator, as illustrated in Figure 15. Moreover it must know at least the locator of the serving UFA_GW. Additionally, the following parameters can also be gathered depending on the actual UFA operations:

- Parameters for 802.21 MIH discovery (Wifi, WiMAX: MIH capability discover, confirm/request calls; 3G UMTS: LLC SAP), PoA, PoS (UFA as Mobility Manager), MIIS (Static Information Base),
- Multihoming policies,
- L or HIT of DHCP server,
- DNS, RVS or other local naming service locator (it can resolve from FQDN to locator or to HIT of MIH services, UFA_GW, DHCP server, etc.),
- Bootstrapping parameters of security protocols (e.g. IPsec PAD and SPD).

Annex C describes the IP acquisition methods recommended for non-3GPP access networks in case of the I-WLAN scenario. The enumerated methods can not be used in UFA, because there is no PDG tunnel establishment in UFA. The natural and common IP acquisition solution is the usage of DHCP or DHCPv6 [25] protocols. The UFA_GW can act as a DHCP server or as a DHCP relay.

Note that when acting as a DHCP relay, DHCPv6 Prefix Delegation (DHCPv6-PD) might also be used by the operator to manage IPv6 prefix allocations. Classical DHCPv6 is typically focused upon parameter assignment from a DHCPv6 server to an IPv6 host running a DHCPv6 protocol stack. DHCPv6-PD however is aimed at assigning complete subnets and other network and interface parameters from a DHCPv6-PD server to a DHCPv6-PD client. The following supplemental alternatives also exist for bootstrapping MNs and UFA_GWs:

- IPv6 Neighbor Discovery,
- IPv6 Secure Neighbor Discovery (RFC 3971),
- DNS, DNSsec,
- HIP BEX (using a HIP-based approach for configuration provisioning in a novel, CFG parameter),
- Diameter for UFA_GW from the network.

After the bootstrapping of the MN, the MN and the UFA_GW execute the HIP BEX for HIP level access authorization, i.e., mutual authentication of the MN and the UFA_GW and negotiation of the IPsec SA pair.

![Diagram of bootstrapping the MN, and HIP-level attachment procedure](image)

**Figure 15: Bootstrapping the MN, and HIP-level attachment procedure**

During HIP BEX, the MN's access authorization can be checked by the home (or a local) ER server because it knows the expected HIT_{MN} from the home server's EAP-Success message, and the MN proves to know hIK. The home (or local) ER's authenticity is proved to the MN by using the correct hIK. The MN checks the freshness of the reply using a sequence number that is known only by the MN and the home (or local) ER server. The UFA_GW is authorized by the MN, because it proves to be in trust relationship with the home (or local) ER server. HIP provides integrity, message-origin authentication, and freshness for I2 and R2 messages.

Note that further master session keys (hMSKs) could be derived from hRK. This could replace the Diffie-Hellman key exchange during HIP BEX, because the MSKs could be used to calculate transient session keys for the HIP and IPsec associations between the MN and the UFA_GW.

After the HIP-level attachment procedure between the MN and the UFA_GW providing secure mutual authentication, two main tasks remain for the last phase of the terminal attachment called the L3 attachment. On one hand 802.21 MIH service and capability discovery, registration, and event subscription must be performed. On the other hand the MN must be registered for the HIT-IP mapping service of the UFA. This service is the Rendezvous Server architecture in this study, however, more sophisticated mapping services (like Hi3) can also be used. This registration is performed by the
UFA_GW on behalf of the MN by mandated action request/reply parameters in I2 and R2 messages of BEX.

![Diagram](image)

**Figure 16: L3 attachment procedure**

### 4.4 Session establishment and maintenance

Session establishment between the MN and a CN is basically a Type 2 Delegation service (MN delegates UFA_GW for BEX and UPDATEs with CNs) where the Delegator, the Delegate and the CN are the MN, MN's UFA_GW and the CN, respectively. If the CN is also an MN, then the HIP and IPsec association is established with the UFA_GW of the CN, and CN is notified using HIP Notification in order to create HIP association states with the MN in the CN. The UFA_GW creates a mapping table entry for the MN and the CN in order to route their traffic into the appropriate IPsec tunnels. Note, that in order to avoid maintenance of unnecessary states in HIP hosts (and in order to stick to the basic HIP considerations providing DoS resistance) it is important, that MN-UFA connection request must be sent only in I2 and the AUTH CN must be sent only in R2. I1 and R1 messages are both simple HIP BEX messages containing only the standard HIP parameters.

![Diagram](image)

**Figure 17: Session establishment and maintenance procedures in the 802.21-HIP-SIP UFA integration scenario**

#### 4.4.1 Non-SIP applications establishment

After the establishment of the HIP session between the MN and the CN, the MN is able to send the initialization packet of the remote non-SIP service or application running on the CN. This packet is a HTTP GET message if a HTTP-based service is under requisition (e.g., browsing a web-site stored on the CN or applying for a Video-on-Demand show hosted also on the CN). In case of successful service initialization an acknowledge packet is usually sent to the MN from the CN (this is a 200 OK message.
in case of the above examples). Of course any other kind of non-SIP applications and services (FTP, P2P file sharing, instant messaging, etc.,) can be used in this way; the only restriction is that the CN must also be HIP and UFA compatible.

4.4.2 SIP applications establishment

After the establishment of the HIP session between the MN and the CN, the MN is able to send to SIP INVITE message to the CN, Figure 18.

The U-CSFCF is the outbound proxy for the MN. IP packets with SIP signalling from the MN are sent to the UFA_GW (@IP destination of the U-CSFCF). After treatment of SIP signalling by the U-CSFCF a new IP packet is created to the CN via the S-CSFCF.

After SIP exchanges and media negotiation, media plane is set up by MN and CN. IP traffic is routed through the UFA-GW. Admission control and IP filtering is made by the UFA_GW for security reasons:

- IP spoofing,
- Ports filtering according to SIP signalling.

During session establishment, the UFA_GW could reduce the number of media because of lack of resources and shall store the initial application negotiated between the two users. Thus, it will be able to initiate a session upgrade when resources will become available.

Figure 18: SIP Session establishment procedure in the 802.21-HIP-SIP scenario, part I
4.5 Mobility procedures

4.5.1 Handover initiation

The handover is initiated by the UFA_CL module of the S_UFA_GW due to the monitoring of link layer events of the MN through the MIH framework. The UFA_CL module registers the observation of specific link layer events in the MN. It configures thresholds for specific QoS metrics of the MN’s traffic. The UFA_CL is notified about L2 events of the MN with periodic MIH_Link_Parameters_Report indication messages, and at link quality degradation, with the MIH_Link_Going_Down indication.

Figure 20: Handover initiation
4.5.2 Handover preparation phase

Figure 21 summarizes the MIH-based handover preparation phase based on the 802.21 protocol, in order to decide about the handover of the MN. The following MIH protocol phases must be performed:

Information query:
First, the UFA_CL in the S_UFA_GW collects static network information about possible candidate access networks for the MN. Its local database MIH IS database or remote MIH IS in the UFA core network can provide the necessary information about candidate L2 PoAs.

Resource availability check:
Then the UFA_CL queries the available QoS resources in the candidate target networks. If the MN may assist in the decision, then first, the UFA_CL of the S_UFA_GW sends the list of available networks to the MN, and the UFA_CL of the MN narrows this list to its preferred target networks.

This procedure is performed with the MIH_MN_HO_Candidate_Query primitives.

After this, the UFA_CL of the S_UFA_GW collects all dynamic resource availability information from the possible target L2 PoAs using the MIH_N2N_HO_Query_Resources primitives.

Decision:
Finally, the UFA_CL of the S_UFA_GW decides the target network (L2 PoA) for the MN. The 802.21 protocol does not define the decision method. In the handover decision phase, the UFA_CL of the S_UFA_GW selects the target L2 PoA and T_UFA_GW to which the S_UFA_GW will hand off all or part of the sessions of the MN. Note, that in use-case 2 it is possible to execute per application mobility, i.e., only some part of the sessions of the MN may be arranged to flow through the target network. Hence the UFA_CL of the S_UFA_GW selects the MN’s sessions that must be hand off to the target network in order to maintain the QoS of the ongoing sessions or to behave to some service policies.
HIP level handover preparation

The necessary contexts are then proactively established in the target network and the affected peers of the MN.

Prerequisites for HIP and IPsec context establishment

The T_UFA_GW must be registered to the S_UFA_GW’s Type 1 Delegation service, to delegate HIP and IPsec association establishment. The T_UFA_GW authorizes the S_UFA_GW for the establishment of HIP and IPsec connections with peers in T_UFA_GW’s name, and then send the contexts to the T_UFA_GW. Hence, the number of HIP BEX procedures is reduced, and replaced by HIP Updates.

The S_UFA_GW or the MN must subscribe to T_UFA_GW’s Type 2 delegation service. Hence, the T_UFA_GW can update the MN’s location for all the ongoing sessions and services that were affected by the handover, i.e., update the CNs, UFA_GW of CNs, RVS of the MN.

First, the contexts above the link layer are established. HIP and IPsec contexts are created proactively in the T_UFA_GW, the MN, the CNs, and the RVS of the MN. Due to the HIP handover preparation procedure, the sessions that are handed off to the target network are directed from the CNs to the T_UFA_GW. However, the T_UFA_GW still routes this traffic to the MN through the S_UFA_GW because it might take some time to establish L2 connection with the MN through the target network. The sessions that are not handed off remain unchanged, and are illustrated with dotted double-arrows in the figure. Furthermore, in this phase, the SDP contexts could also be updated in the MN and the CNs for SIP sessions. We propose to perform context establishment for transparent per application handovers. Hence, subscriptions to new network services in the target network, such as 802.21 registrations, event subscription should be made after the handover completion.

We present in the followings in details our proposal for the steps of the HIP level handover preparation procedure. Figure 22 depicts the first part of the HIP level handover preparation that is
needed to establish IPsec and HIP states between the T_UFA_GW and new communicating peers of the T_UFA_GW that will appear soon due to the handoff of MN's sessions. Figure 23 illustrates the second part of the handover execution process where the T_UFA_GW updates the name of the MN the communicating peers of the MN to route the MN’s traffic to the T_UFA_GW. In order to support per application handoffs, the peers (CN server, UFA_GWs of CNs) establish new HIP states for the MN instead of overwriting the old ones that pointed to the IPsec SA with the S_UFA_GW. Hence traffic mapping policies can decide based on the traffic type, whether to use the IPsec SA ending at the T_UFA_GW or the S_UFA_GW.

**HIP handover preparation (Part 1)**

The handover execution is triggered by the *HIP UPDATE: Type 2 Mandated Action Request for handing off the MN* message. In this message the S_UFA_GW sends to the T_UFA_GW the HITs of the MN, the type 2 delegation certificate chain of the MN authorizing the S_UFA_GW, the HITs of active peers of the MN, i.e., the CN servers, the UFA_GWs of the CNs and the RVS. The acknowledgment to this message is present in Figure 23. The two last HIP messages are the acknowledgments completing the 3-way handshake of HIP control. The *HIP UPDATE: Type 2 Mandated Action Response for handing off MN* message signals for the S_UFA_GW that the L3 states are pre-established for handing off the decided sessions of the MN.

After the reception of the *HIP UPDATE: Type 2 Mandated Action Request for handing off the MN* message, the T_UFA_GW checks whether it has HIP and IPsec associations with the enumerated UFA_GWs, the RVS, the CN servers, and the MN. If any association is missing, the T_UFA_GW initiates a *HIP UPDATE Bulk Type 1 Delegation Action Request* to its delegate, the S_UFA_GW, to establish the IPsec and HIP associations for the T_UFA_GW and the missing peers. The S_UFA_GW creates IPsec and HIP states for the T_UFA_GW at every missing peer using *HIP UPDATE Type 1 Mandated Action Request and Response messages to Create HIP and IPsec states for the T_UFA_GW*. *HIP UPDATEs* messages in the figure are part of the 3-way handshaking of HIP. When the IPsec and HIP states are created for the T_UFA_GW in the missing peers the S_UFA_GW responds with a *HIP UPDATE Bulk Type 1 Delegation Action Response* message, enumerating that on which peers were the state establishment successful or unsuccessful.

Now, the T_UFA_GW prepares to accept contexts from the S_UFA_GW, and the S_UFA_GW sends the IPsec and HIP contexts using CXTP protocol’s *Context Transfer Data* and *Context Transfer Data Responses* messages.

When the MN has established SIP and non-SIP applications, the S_UFA_GW, data information of the MN in the transfer context contains also SIP layer information and description of any layer as the UFA_CL manages all the layer of the MN. Please refer to [9] §5.3.3.1 for more information and description of the context transfer between the S_UFA_GW and the T_UFA_GW.
HIP handover preparation (Part 2)

In the second part of the HIP handover preparation procedure, depicted in Figure 23, the T_UFA_GW acts as the Delegate of the MN. It can act in this role, for two reasons.

- It has got the certificate chain authorizing the S_UFA_GW for providing Type 2 Delegation service to the MN in the first message in Figure 22, and it has a Type 2 Delegation service authorization certificate from the S_UFA_GW because the S_UFA_GW had already registered to its Type 2 delegation service.

- The MN can register directly to Type 2 delegation service of the T_UFA_GW in HIP UPDATE Type 1 Mandated Action Response to Create HIP and IPsec states for the T_UFA_GW. In this case the MN have included the Authorization Certificate for the T_UFA_GW to provide Type 2 delegation service for the MN.

The T_UFA_GW creates in the name of the MN a new HIP association entry in the CN servers or UFA_GWs of the CNs, and the RVS of the MN. This HIP association entry maps the traffic destined for the MN to the IPsec ESP tunnel between the peer and the T_UFA_GW. From now, the peers route the traffic of the MN into the direction of the T_UFA_GW.

When the T_UFA_GW gets the HIP UPDATE Type 2 Delegation, Mandated Response HIP states created for MN message, it updates locally its HIT-based mapping table, i.e., traffic coming from the peers for the MN will be mapped to the IPsec tunnel having the S_UFA_GW on the other side. The mapping table entries for the opposite direction must also be prepared in the T_UFA_GW.

When the S_UFA_GW get to know that the HIP and IPsec contexts are established for handing off the MN’s sessions, it also updates its local HIT-based traffic mapping table. The traffic coming from the MN, related to the sessions that will be moved soon, must be mapped to the IPsec tunnel that has the T_UFA_GW on the other side.
Traffic mapping policy management to support multi-access services and per application mobility

The management of traffic flow routing policies to provide per application mobility and multi-access services for use-case 2 are controlled also with HIP parameters in our proposal. It is the UFA-CL module of the S_UFA_GW that basically brings decisions to handoff MN’s sessions. However, MN may also request to hand off sessions.

The S_UFA_GW may send updated traffic mapping policy descriptors to the T_UFA_GW within the HIP Update Type 2 Mandated Action Request for handing off MN request message. The MN might trigger the policy update by HIP UPDATE Type 2 Delegation Action Request.

The T_UFA_GW then should update the traffic mapping policies in the CN servers, and the UFA_GWs of the CNs and also in the MN, with HIP UPDATE Type 2 Delegation, Mandated Requests. Hence the MN’s communicating peers map according to the new mapping rules their ongoing sessions with the MN, to the IPsec tunnels via the S_UFA_GW or via the T_UFA_GW.

4.5.3 Handover execution phase

L2 handover execution procedure: option 1

After L3 context establishment, proactive L2 context establishment is performed, preparing the target network to transport MN’s flows. The UFA_CL of the S_UFA_GW prepares resources on the target L2 PoA and T_UFA_GW for the MN. Note that the figure is simplified; the L2 PoA is part of the UFA_GW. Hence MIH_N2N_HO_Commit request and response messages are sent to the T_UFA_GW instead of the target L2 PoA.

When the T_UFA_GW informs the S_UFA_GW that resources concerning all the layers are prepared in the target network, the UFA_CL in the S_UFA_GW directs the MN to perform L2 attachment to the target network.

In use-case 1, hard handover must be performed because the MN is a single-interface device. In use-case 2 soft handover is performed, moreover, the HIT-based mapping tables are updated in the...
MN to route the moved traffic flows into the IPsec tunnel that has been established with the T_UFA_GW in the handover execution phase.

The following 802.21 MIH primitives for L2 QoS resource preparation are used in the handover decision phase:

- **MIH_MN_HO_Commit**: Command used by MN to notify the serving network of the decided target network information
- **MIH_N2N_HO_Commit**: Command used by a serving network to inform a target network that an MN is about to move toward that network, initiate context transfer (if applicable), and perform handover preparation.

L2 fast re-authentication procedures, such as the EAP Re-authentication Protocol (ERP) [21], are triggered after the MN gets the MIH_NET_HO_Commit response message, before or after performing the physical handoff. L2 fast re-authentication methods may be access technology dependent. Some fast L2 re-authentication techniques for L2 handovers are summarized in Annex E. If all access technologies use EAP-based authentication, ERP can be applied in an access technology independent way to provide fast L2 handovers.

SIP handover execution procedure: option 3

When the MN has established SIP and non-SIP applications, at least one SIP application, the handover execution of the MN could be executed by the SIP the layer. A SIP re-INVITE message is sent between the U-CSCF of the S_UFA_GW to the MN to execute the HO. The SIP re-INVITE message contains information on all layers of the MN. For more detail on the SIP HO execution procedure, please refer to [9] §5.3.3.1. Compared to the procedure defined on the Figure 24, the SIP re-INVITE, 200 OK and ACK messages replace the MIH_NET_HO_Commit request and the MIH_NET_HO_Commit response. The objective of option 3 procedure is to reduce interruption session delay when the SDP of SIP applications has to be changed because the T_UFA_GW could not offer same radio resources to the MN as the S_UFA_GW. The risk, if the MN executes the SIP re-INVITE message after the handover, to update the SDP, is that the QoS of the SIP session could be degradad.

If the T_UFA_GW could offer more capacity to the MN, the same procedure could be executed. Nevertheless the MN could wait for the MN completion to update the SDP.
4.5.4 Handover completion phase

Figure 26 illustrates the handover completion phase, which is initiated when the MN physically attaches to the target PoA. At this time the bootstrapping parameters are already known by the MN.

The MN signals with the MIH_MN_HO_Complete request message to the source L2 PoA (and the source UFA_GW) that they can release the resources maintained for the MN’s sessions. In use-case 1, all QoS resources maintained for the MN are released in the source L2 PoA and S_UFA_GW. In use-case 2 partial soft handover of SIP and non-SIP sessions may be supported. The UFA_CL module (MIH User) in the MN may in this case be aware of releasing only part of the MN’s QoS resources. Note, that in this case MIH_MN_HO_commit primitive could be used instead of MIH_MN_HO_complete, leading to the reduction of the occupied QoS resources in the source L2 PoA and S_UFA_GW for the MN’s sessions.

In use-case 1, the handover completion messages are routed through the T_UFA_GW, as illustrated in the figure. In use-case 2, the handover commit messages reach directly the S_UFA_GW from the MN. Note that another possibility for use-case 2 is that the UFA_CL module of the S_UFA_GW reduces the QoS resources of the MN by local MIH commands.

The routing of traffic flows must also be updated for the MN. When the S_UFA_GW gets the HO complete or MN HO commit form the MN, it updates for the MN the HIT-based traffic mapping table entries of the MN in the T_UFA_GW, using HIP update with Type 2 Delegation – Mandated request. Hence, the T_UFA_GW routes all traffic destined to the MN through the direct IPsec tunnel. After getting the Type 2 Delegation – Mandated Response from the T_UFA_GW, the S_UFA_GW deletes the HIT-based traffic mapping table entries for the transferred sessions of the MN.

The figure also depicts that some traffic could remain routed through the S_UFA_GW. Naturally, this is only valid in use-case 2.
After the completion of HIP handover, in any use cases of applications establishment, the T_UFA_GW has not to inform the S-CSCF that the MN has changed its location under the coverage of a new UFA_GW in order to receive new IMS incoming calls.

Figure 26: Handover completion phase.
5 Ultra Flat Architecture integration scenario no.2: 802.21 in combination with PMIP and SIP

5.1 Proxy MIP and UFA Integration Overview

Proxy Mobile IPv6 protocol is intended for providing network-based IP mobility management support to a Mobile Node (MN), without requiring the participation of the MN in any IP mobility related signaling. The mobility entities in the network will track the MN's movements and will initiate the mobility signaling and set up the required routing state.

The core functional entities in the NETLMM infrastructure are the Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG). The LMA is responsible for maintaining the MN's reachability state and is the topological anchor point for the MN's home network prefix(es). The MAG is the entity that performs the mobility management on behalf of a MN, and it resides on the access link where the MN is anchored. The MAG is responsible for detecting the MN's movements to and from the access link and for initiating binding registrations to the MN's LMA. There can be multiple LMAs in a Proxy Mobile IPv6 domain each serving a different group of MNs. The architecture of a UFA and PMIP is shown in Figure 27, including the 802.21 entities.

![Figure 27: UFA and PMIP Architecture](image-url)
5.2 Attachment procedure

5.2.1 Registration / Authentication procedure

In Annex A we presented the classical procedure for registration/authentication to access network and IMS levels as standardized in 3GPP. In that procedure, five steps are necessary to access an IMS-based service:

- ATH_1: Registration/authentication to Access Network,
- ATH_2: Bearer establishment for SIP signaling,
- ATH_3: IP address acquisition,
- ATH_4: P-CSCF discovery,
- ATH_5: Registration/authentication to IMS.

In this section, we define the registration/authentication procedure for UFA for the PMIP-SIP combined scenario, by analysing how each step performed in the classical procedure will be performed in UFA.

ATH_1: Registration/authentication to UFA on the Access Network level

It is proposed here to use EAP over IKE2v2 protocol to support the AKA authentication method. The same flow chart used for I-WLAN [1] can be used here.

During this phase, an IP address could be allocated to the MN with using IKEv2 configuration options. Also an IPsec Tunnel is build during this phase based on IKEv2.

ATH_2: Bearer establishment for SIP signaling

This phase remains the same for UFA and is necessary.

ATH_3: IP address acquisition

The MN has already acquired its IP address during ATH_1. This step is not necessary.

ATH_4: U-CSCF discovery

The MN discovers the U-CSCF address in the UFA GW based on DHCP (RFC[2131], RFC[3361], RFC[2132], RFC[3263] and DNS. If U-CSCF address is transmitted to the MN during ATH_1 then this step is not necessary.

ATH_5: Registration/authentication to UFA on the IMS level

For UFA, in ATH_5, we propose a method similar in its principles to the one presented just above with a single round of SIP REGISTER / 200 OK. The difference concerns the authentication of the MN by the UFA_GW instead of the S-CSCF. This necessitates some mapping actions:

- During ATH_1, the UFA_GW stores the mapping between IMSI and the IP address allocated to the MN.
- When the S-CSCF receives the SIP REGISTER message including the user IMS identity (IMPI), it asks the HSS to send to it the IMSI corresponding to the IMPI.
- The S-CSCF sends back in the SIP 200 OK message: IMSI received from the HSS, IMPI and IP received in the SIP REGISTER.
- When the UFA_GW receives the SIP 200 OK message it compares the received information with the one stored during ATH_1, if they are the same then the user is authenticated.

The IPsec tunnel built during ATH_1 can be used to secure all data exchanged between the MN and UFA_GW including SIP signaling.
5.2.2 PMIP initialisation procedure

Thanks to the registration and authentication procedure described in section 5.2.1, the MN acquired an IP address and all other layer 3 parameters after it has been authorized to attach to the network through an UFA_GW. More precisely, UFA_CL of the serving UFA_GW has created a user context to manage the MN.

UFA_CL has to inform the MAG entity about the attachment of a new MN.
For updating the LMA about the current location of the MN, the MAG sends a Proxy Binding Update message to the MN's LMA. Upon accepting this Proxy Binding Update message, the LMA sends a Proxy Binding Acknowledgement message including the MN's home network prefix(es). It also creates the Binding Cache entry and sets up its endpoint of the bi-directional tunnel to the MAG.

The MAG on receiving the Proxy Binding Acknowledgement message sets up its endpoint of the bi-directional tunnel to the LMA and also sets up the forwarding for the MN's traffic. At this point, the MAG has all the required information for emulating the MN's home link. It sends Router Advertisement messages to the MN on the access link advertising the MN's home network prefix(es) as the hosted on-link prefix(es).

The MN, on receiving these Router Advertisement messages on the access link, attempts to configure its interface using either stateful or stateless address configuration modes, based on the modes that are permitted on that access link as indicated in Router Advertisement messages. At the end of a successful address configuration procedure, the MN has one or more addresses from its home network prefix(es).

After address configuration, the MN has one or more valid addresses from its home network prefix(es) at the current point of attachment. The serving MAG and the LMA anchor also have proper routing states for handling the traffic sent to and from the MN using any one or more of the addresses from its home network prefix(es).

The LMA, being the topological anchor point for the MN's home network prefix(es), receives any packets that are sent to the MN by any node in or outside the Proxy Mobile IPv6 domain. The LMA forwards these received packets to the MAG through the bi-directional tunnel. The MAG on other end of the tunnel, after receiving the packet, removes the outer header and forwards the packet on the access link to the MN. The MAG acts as the default router on the point-to-point link shared with the MN. Any packet that the MN sends to any correspondent node will be received by the MAG and will be sent to its LMA through the bi-directional tunnel. The LMA on the other end of the tunnel, after receiving the packet, removes the outer header and routes the packet to the destination.
5.3 Session establishment and maintenance

For the session establishment and maintenance of applications for the integrated scenario PMIP-SIP, all the procedures could be applied on use case 1 and use case 2.

5.3.1 SIP applications

Using cross layer mechanism, UFA allows the access layer to interact with the control layer with the implementation of a new IMS proxy named U-CSCF, controlled by the UFA_CL. Thus, it is able to check locally (within the UFA_GW) whether the negotiated session characteristics and the available access network resources are matching. Therefore, it is to the UFA_GW to choose the right codec for the session since it knows both network and terminal capabilities. This choice is made thanks to QoS preconditions used in SDP (Session Description Protocol) which will be discussed later.

The UFA_GW could also control the user profile to apply a specific policy control according to the user rights. The user profile has been stored in the UFA_GW during the MN registration / authentication procedure; see section 5.2.1 for more information.

Here is a call flow for a service establishment session. Indeed, the call can rarely fail since the terminal chooses among codecs which the network already allowed their transmission.

![Figure 30: Service establishment call-flow – SDP Offer/Answer](image)

The U-CSCF of the UFA_GW implements a major part of the IMS/UMTS procedures. Moreover, it can also modify terminal preferences according to an algorithm that will be discussed later. Then, when it sends back the SDP offer to the terminal, the latter can only the media and codecs which the network has resource availability for. Finally, it can also perform session upgrading (or downgrading) since it knows both terminal and network capabilities.
It is assumed here that a network can choose among codecs only based on their bandwidth whereas the terminal can choose according to the codec support (for instance, if it can decode MPEG-4 or not), bandwidth, etc.

Here is the description of each step. Note that 3 MN/CN exchanges are needed to come to a final SDP. That is why the case when the SDP offer is not contained in the SIP INVITE is not an issue.

- **SDP Offer/Answer**
  - 1: MN initiates a video call towards CN containing a first SDP offer in a SIP INVITE. Preconditions are included in order to indicate that resources are not reserved in both ends.
  - 2: U-CSCF asks the UFA_CL on the available resource for the MN and control the user profile. Based on the UFA_CL answers, U-CSCF (UFA_GW (MN)) modifies the offer since it has only resource for video codec2 and no resources for video for example. It just modifies the order to show its preference and put an RTP port equal to zero to indicate its incapability to support video. It does not delete anything since the UFA_CN and the CN has to know about the complete offer. U-CSCF stores the capabilities for a possible upgrading. SIP INVITE is sent to the S-CSCF.
  - 3: At the S-CSCF, an AS invocation could be done to control the demand. It could control the user profile if needed or route the request to an AS according to the status of the CN for example. For this call-flow, we consider that MN and CN are connected to UFA_GWs under the same S-CSCF in order to simplify the call-flow. We suppose also that both CN and MN are under the same network.
  - 4: U-CSCF of the UFA_GW (CN) interprets the SDP and asks the UFA_CL on the available resource for the CN and control the user profile. Based on the UFA_CL answers, U-CSCF, as MN supports audio and video codec1 (SDP content) and codec2 but network can only provide codec2 (order and RTP port), can assure audio codec2 transmission so it forwards the message as it is received.
  - 5: The CN filters the SDP according to its capabilities. It knows that network can only support audio codec2 but it also filters the rest. In this case, the CN cannot support video codec2. Thus, it removes it from the SDP offer and builds the SDP answer.
  - 6: The U-CSCF of the UFA_GW (CN) knows both CN (deduction) and MN (stored) capabilities. U-CSFC informs the UFA_CL about the SDP selection. The UFA_CL computes bearer configuration for voice codec2, sends it to the CN and put QoS preconditions as reserved on CN side in the SIP 183 message sent to the U-CSCF of the UFA_GW (MN) via the S-CSCF.
  - 7: The S-CSCF proxies the SIP message to the U-CSCF UFA_GW (MN).
  - 8: The U-CSCF of the UFA_GW (MN) deduces CN capabilities and informs the UFA_CL. The latter computes bearer configuration for the final SDP and put QoS preconditions as reserved on MN side and sends it back to the U-CSCF which sends both (SDP and bearer configuration) to the MN.
  - The MN then deduces CN capabilities and stores them (optionally), and configures the bearer locally.
Figure 31: Service establishment call-flow – SDP Confirmation

- **SDP Confirmation**
  - 9-10-11-12: The MN sends back the retained offer for confirmation to the CN.
  - 13-14-15-16: CN receives the confirmation. Moreover, it indicates that resources are reserved for this SDP. Thus, after acquitting, it sends back a **SIP RINGING** indicating that the session is established.

5.3.2 Non-SIP applications
The existing most common Internet applications are not based on SIP protocol for establishing the session. Since these legacy applications, such as HTTP and FTP, are very important, UFA architecture must support them. Therefore, the UFA architecture must use the PMIP protocol to support mobility within these non-SIP applications (as defined in section 5.4).

5.4 Mobility procedures
5.4.1 Handover initiation phase
During the handover initiation phase, due to the deterioration of the wireless conditions or because a new network providing better conditions is available, the UFA mobility management algorithm decides to initiate the handover process to one of the candidate UFA GWs.

Initially, the Mobile Node (MN) is connected to the serving UFA_GW and exchanges traffic with a Correspondent Node (CN) on the Internet or to a service platform. During the handover initiation phase the S_UFA_GW (MIH PoS) configures the serving access interface of the multimode terminal with the set of QoS parameters required for the serving access link (**MIH Link Configure Thresholds**). As a result, the serving access interface will periodically notify the registered MIHUs about its QoS parameters, with **MIH Link Parameters Report** events. Besides these periodical notifications, the serving access interface triggers this event if the configured thresholds are crossed and are no longer satisfied by the wireless interface.

Another possibility is to trigger the **MIH Link Going Down** event when the air link conditions start degrading, and it is predictable that within a certain period of time the connection will be lost. With this procedure, both MN and UFA_GW entities have sufficient information about the serving access interface status in real time and, if necessary, can trigger the HO preparation phase before the link goes down. Both mobile-initiated and network-initiated handovers are supported using this mechanism.
5.4.2 Handover preparation

The handover preparation phase is initiated to prepare the target UFA_GW for the MN handover. During this phase all available information is collected in order to help the selection algorithm in the S_UFA_GW to decide for the target UFA_GW. This phase is constituted by the following sub-phases:

- **Discovery**: During this phase, the list of candidate UFA_GWs is obtained:
  - Thanks to the Information System or local information base of the serving PoS, which collects static information on candidate Point of accesses, such as their identifiers, L2 addresses, accounting information, etc.
  - Thanks to exchange between UFA_GWs.
- **Query**: In this phase, the mobility decision algorithm acquires all QoS metrics for all available candidate UFA_GWs.
Figure 33 illustrates the handover preparation phase for a network-initiated handover using Proxy Mobile IPv6 (PMIPv6). The MN receives packets through the MAG located in the serving network. The Serving PoS queries the Information Server to get information about available neighboring networks (MIH_Get Information).

The Serving PoS sends the MIH_N2N_HO_Query_Resource request messages to different Candidate PoSs (can be more than one) of candidate UFA GWs to query the resources availability at each candidate UFA GW. The Candidate PoSs respond by sending the MIH_N2N_HO_Query_Resource response message to the Serving PoS. The Serving PoS decides to execute a handover to a selected target UFA GW based on the resource availability information of candidate UFA GWs informed by the MIH_N2N_HO_Query_Resource response message. Note that if MN assisted decision is required (performed by the UFA CL of the MN), then the UFA GW can send the list of candidate PoAs to the MN to narrow it by the MIH_Net_HO_Candidate request and responses, before sending out MIH_N2N_HO_Query_Resource requests to candidate PoAs.

![Figure 33: Handover Preparation Phase – Centralized procedure](image-url)
Figure 34 illustrates the handover preparation phase for a network-initiated handover using Proxy Mobile IPv6 (PMIPv6). The MN receives packets through the MAG located in the serving network. The Serving UFA_GW queries the neighboring UFA_GWs (MIH_Get Information) to get information about resources availability. The list of neighbor UFA_GWs could be learnt by the serving UFA_GW by Self Organizing Network mechanisms.

### 5.4.3 Handover decision phase

During the handover decision phase the target network is selected and the radio resources are activated. This phase is constituted by the following sub-phases:
• **Selection:** During this phase, the mobility decision algorithm running either on the network side or in the terminal side, decides for the target network.

• **Commit:** In this phase, the required QoS resources, and all the other required resources for the MN running services are established on the target access network.

The Serving PoS informs the decided Target PoS (where the target MAG is located) of the handover commitment and requests the Target PoS to prepare resources for the incoming MN through sending the MIH_N2N_HO_Commit request message. The Target PoS replies to the result of the handover commitment and resource preparation by sending an MIH_N2N_HO_Commit response message.

Upon receiving the MIH_N2N_HO_Commit request message, the UFA_CL entity in the Target PoS queries the incoming MN’s profile to an AAA server and sends a Proxy Binding Update in order to register the location of the MN in advance. The PMIPv6 client in the Target PoS buffers the packets received from the LMA until the MN attaches to the Target PoS.

The Serving PoS requests the MN to perform handover to the decided Target PoS by sending the MIH_Net_HO_Commit request message. The MN replies with the result of the handover commitment by sending an MIH_Net_HO_Commit response message.

![Figure 35: Handover Decision Phase](image)

### 5.4.4 Handover execution phase mobile-initiated

Upon detecting the MN’s detachment, the PMIPv6 client in the Serving PoS terminates its current binding of the MN via sending a Proxy Binding Update with Lifetime set to 0 and requests the LMA to buffer packets destined for the MN.

Once the MN establishes Layer 2 connection to the Target PoS, the PMIPv6 client in the Target PoS registers the current MN’s location to the LMA by sending a Proxy Binding Update message. The LMA updates its Binding Cache Entry with the Proxy Binding Update message and then replies with a Proxy Binding Acknowledgement message. The LMA forwards the buffered packets.

After receiving the Proxy Binding Acknowledgement message, the PMIPv6 client sends a Router Advertisement message to the MN. The Router Advertisement is constructed with the MN’s information obtained from the LMA. It can be solicited by a Router Solicitation message from the MN or periodically transmitted. The MN configures IP addresses on its interface, which is currently used to connect to the Target PoS, with the received Router Advertisement message. Once the PMIPv6 procedures are completed, the MN receives packets through both MAG and LMA.
Figure 36: Handover Execution Phase mobile-initiated
5.4.5 Handover execution phase network-initiated

L2 handover execution procedure: option 1

In the mobile initiated handover scenario the PMIP protocol is triggered by the MN detention (detected by the MAG), whereas in the network initiated handover scenario the PMIP entity (MAG) is triggered by the 802.21 elements on the network side. Figure 37 illustrates a network initiated handover procedure using PMIP and 802.21 protocols. Initially, the network (Serving UFA Gateway – S_UFA_GW) decides to execute a handover and move the Mobile Node (MN) from the serving access network to a target access network (T_UFA_GW). After deciding to handoff the terminal to a new network, the MIHF at the network side triggers the \textit{MIH\_Net\_HO\_Commit request} message towards the MN to force it to handover to the selected target access network. The MN acknowledges the MIHF at the network side by sending the \textit{MIH\_Net\_HO\_Commit response} message, which thereafter informs the PMIP MAG about the handover procedure. As a result the MAG will start buffering the packets that are being sent to the terminal. The remaining part of the handover process is exactly the same as described in the previous section (section 5.4.4).

![Figure 37: Handover Execution Phase network-initiated – Option 1](image)

SIP handover execution procedure: option 3

When the MN has established SIP and non-SIP applications, the handover execution of the MN could be executed by the SIP the layer instead of the 802.21 messages. A SIP re-INVITE message is sent between the U-CSCF of the S_UFA_GW to the MN to execute the HO. The SIP re-INVITE message contains information on all layers of the MN.

For more detail on the SIP HO execution procedure, please refer to [9] §5.3.3.1.
5.4.6 Handover completion phase

Downlink and uplink data starts flowing through the new access air link and the handover completion phase is triggered. After the PMIPv6 execution, the Target PoS sends the MIH_N2N_HO_Complete request message to the previous Serving PoS. The previous Serving PoS responds to the message with a MIH_N2N_HO_Complete response message.

After the completion of PMIPv6 handover, in any use cases of applications establishment, the T_UFA_GW has to inform the S-CSCF that the MN has changed its location under the coverage of a new UFA_GW in order to receive new IMS incoming calls, Figure 40.
Figure 40: Handover completion phase – SIP registration.
6 UFA integration scenario analysis

The objective of this chapter is to evaluate the two UFA integration alternatives defined in the previous chapter:

1. 802.21 in combination with HIP and SIP,
2. 802.21 in combination with PMIP and SIP.

The performance evaluation of the two scenarios will consider only use case 1, MN with a single interface, as it is the worst case of the MN handover.

6.1 Objectives for the evaluation

The objectives of the evaluation are the following. The numbers in parentheses refer to a given signalling scheme in a given application scenario.

1) For non-SIP applications, comparison of the HIP (1.1) and the PMIP (1.2) based on UFA signalling schemes.

2) For SIP-applications, consider and evaluate option 1 (see Section 3.1): either HIP (2.1) or PMIP (2.2) makes the handover (in the same way as for (1.1) and (1.2)), furthermore after physical handover SIP may update the SDP (QoS) of the SIP session.

SIP re-INVITE procedures have to be added after HO completion of HIP or PMIP, in order to update SDP according to the resources on the T_UFA_GW / candidate L2 PoA.

3) For SIP applications, consider and evaluate option 3, i.e., where SIP re-INVITE replaces 802.21 MIH_Net_HO_commit request and response messages to the MN in order to detach from the S_UFA_GW and attach to the T_UFA_GW. SDP update may be performed before the physical handover thanks to the SIP mobility (re-INVITE) procedure. Otherwise, the HIP (3.1) and PMIP (3.2) procedures remain the same as defined in the previous use case.

The decision engine used for the evaluation is the Multiplicative Analytic Hierarchy Process slightly optimized for our needs. Multi-Criteria Decision Analysis is concerned with the evaluation of a finite number of alternatives under a finite number of criteria by a single or a group of decision makers. The Multiplicative Analytic Hierarchy Process (MAHP)[28], used in our study, is a procedure that facilitates the ranking of alternatives by decomposing the complex matching problem for all criteria to many pairwise comparisons of the alternatives under each criterion. The details of our evaluation process have been published in [29] and [30].
6.2 Decision criteria

Our objective was to find the most relevant criteria for the evaluation of the alternatives. Good criteria are the ones that show well the costs and benefits of the alternatives regarding the business objectives. We defined three main criteria, i.e., provide (1) high performance, (2) high security, and (3) low development and implementation cost. There are fifteen sub-criteria under them, organized in a decision tree, illustrated in Figure 41.

The criteria weights were defined in an iterative process, based on the consensus of five decision makers using direct logarithmic difference assignment and direct weight assignment. Annex F describes in details the input forms that we have used for the criteria weight assignment. In case of the direct weight assignment, the decision makers assign weights or proportions to each criterion. This was applied for the definition of the weights of the main criteria (i.e., low performance cost, high security, easy deployment). In direct logarithmic difference assignment, decision makers assign subjective difference values $\Delta_{j,k,d} = \{-6, \ldots, -2, -1, 0, 1, 2, \ldots, 6\}$ between criteria $j$ and $k$, $j=1..M-1$, $k=j..M$. $M$ is the number of criteria under a given branch of the criterion tree. The logarithmic differences are transformed to subjective preference ratios between criterion pairs, using the following equation:

$$ r_{j,k,d} = 2^{\gamma \Delta_{j,k,d}} $$

$\gamma = 1$ was used for each criterion. E.g., if $\Delta_{j,k,d} = 6$, then criterion $j$ is 64 times more important than criterion $k$ in decision maker d’s opinion ($d$ is the index of decision makers, $d=1..D$). Given the
subjective preference ratios, we can calculate the terminal scores of the criteria $j$ ($t_j$), $j=1..M$, with the aggregation function:

$$t_j = \prod_{k=1}^{M} \prod_{d=1}^{D} r_{j,k,d}^{p_{k,j,d}/M}$$

$p_{k,j,d}$ is the weight of the decision maker, $D$ is the number of decision makers. Finally, the normalized weight ($c_j$) of each criterion can be calculated with the following normalization:

$$c_j = \frac{t_j}{\sum_{k=1}^{M} t_k}$$

These calculations must be done to assign weights to the edges in each branching point of the criteria tree. Hence each main criterion, sub-criterion, and sub-sub-criterion gets a weight.

The obtained criteria weights are presented in the first column of Figure 41. As it can be seen from the weights, the dominating sub-criteria under the three main criteria are the low real-time service interruption delay due to inter UFA GW handovers; the mutual authentication, signalling and user data protection between the MN and the UFA GW; and the low number of additional modules to deploy in the MN in the control plane and user plane, respectively. Each message overhead sub-criterion under the performance criterion contains five sub-sub-criteria that are not illustrated in the figure. Those criteria break down to different parts of the UFA network the signalling message overheads, and the weights of these criteria tell about the importance of the low message overhead on a given network part. The message overhead criterion for the network part between the MN and the UFA GW (i.e., network parts I and VII in Figure 43 presented later) dominates the five sub-sub-criteria. The assigned weights for different network parts are detailed in Annex F.

The criterion tree presents the hard constraints ($P_{min}$, $P_{max}$) for every criterion, which was defined based on specifications, such as the maximum real-time service interruption delay (200 ms), or by the judgement of the authors. The scale type and progression factor (gamma) of the performance category assignment scales were carefully defined for each criterion in order to reflect the quality of experience differences between different criterion metric values. The applied scale types and parameters ($g_{min}$, $g_{max}$, $\gamma$, $P_{min}$, $P_{max}$) for performance category assignment are presented in Figure 41.

Figure 42 illustrates all possible performance category assignment types when using geometrical scales. In the illustration $g_{min}=20$ and $g_{max}=120$, giving the starting and ending of the geometrical scale, and $\gamma=0.5$, giving the shape of the scale. The following hard constraints were set for this illustration. For Type-1 and Type-4 functions, $P_{min}=g_{min}$ and $P_{max}=200$. For Type-2 and Type-3 functions, $P_{max}=g_{max}$, and $P_{min}=0$. It can be seen that the performance categories can take the integer values $v=1..7$. However, if the alternative performs outside the hard constraints, then $v=0$. To give some examples, a criterion requiring low handover delay might use Type-2 or Type-3 scales, depending on the decision maker. Both scale assign better grades for lower delays. A requirement for the support of some security features should use Type-1 or Type-4 scales, where “non support” and “support” of a security control should be expressed with $P=0=g_{min}$ or $P=1=g_{max}$, respectively. A criterion for low message overhead may use a Type-3 scale, to reflect the super-linearly increasing system utilization by higher number of messages.

Some of the main requirements of the UFA, such as high scalability, self-configuring and self-optimizing network were not included in our evaluation due to the following reasons. Good scalability is mainly ensured by the structure of the architecture, and influenced by the user traffic. Hence, the signalling schemes would not make much difference under the scalability criterion. The other previously mentioned criteria are difficult to evaluate in this phase of the project.
6.3 Network model for performance evaluation

The analysis of the alternatives under performance criteria is based on the network model presented in Figure 43. It is composed of the MN, the UFA_GWs in charge of MN or CN attachment and the UFA core nodes. We suppose in our model that all UFA equipments are linked to a full mesh IP network. We analyzed two different network scenarios, i.e., in the first scenario (S1) the CN is a server, e.g., an IMS IPTV server or a HTTP server, in the second scenario (S2) the CN is a MN attached to an UFA_GW.

The parameters of the model are summarized in Table 2. In case of fixed settings of the network model, the fixed delay values were used. In case of evaluations with running access network delay (see dMN, dCN delay intervals), we used the given intervals within our calculations.
### Table 2: Parameters used in our network model.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Delay [ms]</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dMN</td>
<td>[1..100] 10</td>
<td>access network delay bw. MN and UFA_GW or L2PoA</td>
</tr>
<tr>
<td>dCN</td>
<td>[5..100] 10</td>
<td>access network delay bw. CN and UFA GW (dMN = dCN)</td>
</tr>
<tr>
<td>dt</td>
<td>[5..50] 30</td>
<td>IP network delay bw. UFA GW of the MN and the UFA core nodes</td>
</tr>
<tr>
<td>dcore</td>
<td>10</td>
<td>delay bw. the UFA core nodes</td>
</tr>
<tr>
<td>dU</td>
<td>20</td>
<td>delay bw. S_UFA_GW and T_UFA_GW and local AAA proxy</td>
</tr>
<tr>
<td>dcore,CN</td>
<td>S1:dcore S2:dt</td>
<td>delay bw. UFA core elements and the UFA GW of the CN</td>
</tr>
<tr>
<td>dU,CN</td>
<td>S1,S2:dt</td>
<td>delay bw. the S_UFA_GW or T_UFA_GW and the CN (or CN’s UFA_GW)</td>
</tr>
<tr>
<td>dL2,conf</td>
<td>50</td>
<td>L2 attachment delay of the MN to a L2 PoA</td>
</tr>
</tbody>
</table>

### 6.4 Features of the alternatives influencing the evaluation under different criteria

In this part we summarize the properties of the alternatives regarding the three main criteria.

Easy deployment is one of the main criteria. We introduced the following measure for deployment complexity. Assuming a default TCP/IP stack in each UFA node, which supports MIP and IPsec, we counted the surplus protocol/functional modules in user and control plane in the MNs, UFA_GWs, and UFA core network. Table 3 summarizes the modules needed in the UFA nodes for the two combined signalling schemes.

### Table 3: Surplus protocol modules for the alternatives beyond the TCP/IP stack.

<table>
<thead>
<tr>
<th></th>
<th>HIP</th>
<th>PMIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. MN ’s control plane</td>
<td>TCP/IP, HIP, SIP, 802.21, UFA-CL, EAP, ERP</td>
<td>TCP/IP, IKEv2, SIP, 802.21, UFA-CL, EAP, ERP</td>
</tr>
<tr>
<td>2. MN’s user plane</td>
<td>TCP/IP</td>
<td>TCP/IP</td>
</tr>
<tr>
<td>3. UFA_GW’s control plane</td>
<td>TCP/IP, HIP, SIP, 802.21, UFA-CL, EAP, ERP</td>
<td>TCP/IP, IKEv2, MAG, SIP, 802.21, UFA-CL, EAP, ERP</td>
</tr>
<tr>
<td>4. UFA GW’s user plane</td>
<td>TCP/IP</td>
<td>TCP/IP</td>
</tr>
<tr>
<td>5. UFA core components (control and user plane)</td>
<td>TCP/IP, HIP capable DNS, RVS, MIIS, EAP, ERP</td>
<td>TCP/IP, LMA, MIIS, EAP, ERP</td>
</tr>
</tbody>
</table>

The security features of the alternatives are summarized in Table 4. Security criteria are measured with performance values 1 when the given security feature is supported by the signalling scheme, and 0 for non support of the security service. HIP and PMIP based schemes apply HIP and IKEv2, respectively as security control protocol. Both alternatives use IPsec tunnels for the protection of signalling and user traffic between the MN and the UFA_GW. HIP based signalling scheme also establishes IPsec tunnels within the UFA network domain, e.g., among the UFA_GWs or between the UFA_GWs and the RVS in the core.

### Table 4: Security features of the HIP and PMIP based signalling schemes.

<table>
<thead>
<tr>
<th></th>
<th>HIP</th>
<th>PMIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>mutual authentication bw. the MN and the UFA_GW</td>
<td>HIP BEX (ERP)</td>
<td>IKEv2 (ERP)</td>
</tr>
<tr>
<td>signalling protection bw. the MN and the UFA_GW</td>
<td>HIP and IPsec</td>
<td>IKEv2 and IPsec</td>
</tr>
<tr>
<td>user data protection bw. the MN and the UFA_GW</td>
<td>IPsec</td>
<td>IPsec</td>
</tr>
<tr>
<td>DoS resistance of the UFA_GW</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>MiTM resistance bw. the MN and the UFA_GW</td>
<td>true</td>
<td>true</td>
</tr>
</tbody>
</table>

The performances of the alternatives under the message overhead criteria are measured with the number of required messages for one successful network attachment, session establishment and
handover, respectively, at different parts of the network. Furthermore, the service interruption delay due to inter UFA_GW handovers and the handover preparation delays are calculated using the sum of the products of the related signalling messages and the one-way delay of the network parts where the message is transmitted.

The message numbers of the signalling schemes under these aspects is detailed in Table 5. The network parts are illustrated in Figure 43. Annex G contains the detailed message traces for each signalling scheme and application scenario. The control messages are mapped to different network parts of our network model.
Table 5: The signalling demands on different network parts given in number of messages from different aspects for the evaluation of the performance cost sub-criteria.

<table>
<thead>
<tr>
<th>Network parts</th>
<th>HIP (1.1)</th>
<th>PMIP (1.1)</th>
<th>HIP (2.1)</th>
<th>PMIP (2.1)</th>
<th>HIP (3.1)</th>
<th>PMIP (2.1)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scenario 1: CNs are also MNs</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messages causing service interruption delay</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average number of messages for one L2/L3 (re-)attachment</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messages causing handover preparation delay</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average number of messages for one session establishment</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Scenario 2: CNs are servers in the core network</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messages causing service interruption delay</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average number of messages for one L2/L3 (re-)attachment</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Messages causing handover preparation delay</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average number of messages for one session establishment</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Notes</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2010 Eurescom participants in study P1857  EDIN 0586-1857
6.5 Evaluation results

Terminal scores of the alternatives under the defined criteria set and weights

Figure 44 shows the terminal scores of the alternatives under the main and sub-criteria for both network scenarios.

The weights of the criteria and the network parameters were fixed as given in Figure 41 and Table 2. In this evaluation the following assumptions are supposed. The explanation of the values can be found in Annex G.

- For HIP and PMIP based signalling schemes:
  - PL2full=1 (i.e., full EAP-AKA authentication is always needed during attachment or re-authentication with a L2 PoA),
  - Ncn=1 (i.e., the number of CNs of an MN is one),
  - Pmiis=1 (i.e., the S_UFA_GW always needs to ask information from the MIIS for each handover decision),
  - Ncandidates = 1 (i.e., only one possible target L2 PoA/T_UFA_GW is asked about its available resources)
  - PSDPupdate=1 (i.e., SIP sessions always need SDP update due to the handoff to a new access technology or due to changing resources on the next L2 PoA or T_UFA_GW),

- For HIP based signalling scheme:
  - IndTufa=1,
  - PT1mn=1,
  - PT1rrvs=1,
  - PT1cn=1,
  - PT2rrvs=1,
  - Phipmncn=1, and
  - Phipufacn=1.

This means the worst case scenario, because with these values no previously established HIP and IPsec associations are supposed among the UFA network entities except the ones created during MN’s attachment to the UFA_GW.

The overall terminal scores of the signalling schemes can be seen under the “Objective” criterion. The main result of the evaluation can be read from the two subfigures:

- HIP is slightly better than PMIP based alternative. This is mainly due to the fact that it is better in deployment and security.

- HIP and PMIP Option 1 scenarios (2.1 and 2.2) fail due to the fact they induce a real-time session interruption delay greater than 250 ms. In fact PMIP (2.2) fails also when we set dMN and dCN in the network model to 0 ms, i.e., we assume 0 transmission delay between the MN/CN and its UFA_GW. HIP (2.1) and PMIP (2.2) could be considered to be used for non real-time SIP applications (e.g., instant messaging).

- There is negligible difference between the “CNs are MNs” and the “CNs are servers” scenarios, illustrated by the upper and the lower subfigures, respectively.

In the subfigures, the three criteria above the “Objective” criterion are the main criteria, i.e., the performance, security and deployment. In case of the “CNs are MNs” network scenario PMIP is slightly better than HIP. However, in case of “CNs are servers” network scenario, HIP performs slightly better than PMIP. This is true both when (1.1) is compared to (1.2), or (3.1) is compared to (3.2).

Why HIP is better than PMIP is due to the fact that HIP provides built-in DoS resistance that can be parameterized based on the existing threats in the network, to protect the UFA_GWs from malicious MNs. Furthermore, HIP based alternative requires one less surplus module in the control planes of the MNs and the UFA_GWs. HIP module is responsible both for the mobility and the security control,
while in PMIP based scenario this is performed by two modules, i.e., the IKEv2 and the PMIP or MAG.

It is worth to mention that there are big differences between the alternatives regarding the number of handover preparation messages, but in the definition of the performance categorization scale of this criterion we supposed that we do not differentiate the alternatives, which perform under 1 second. I.e., if the handover preparation delay is below 1 second, the alternative is placed in the highest category (v=7). The performance category values decrease to 0 using type-3 geometrical scale, within the range of 1 and 2 seconds.

Figure 44: Terminal scores of the alternatives in the two network scenarios.
One solution to reduce the importance of the handover preparation delay criteria, is for the S_UFA_GW to anticipate the handover of the MN. When an S_UFA_GW controls plural radio cells, it could evaluate the movement and the velocity of the MN to select the relevant Target_UFA_GW to execute the handover.

![Figure 45: Terminal scores of the alternatives under the two network scenarios, with smoother pre-assumptions.](image)

**Figure 45: Terminal scores of the alternatives under the two network scenarios, with smoother pre-assumptions.**
Figure 45 shows the terminal scores for the alternatives, when we make smoother pre-assumptions regarding the probabilities of different events. In this case the assumptions were the followings:

- for HIP and PMIP based alternatives: Pmiis=0.5, Ncandidates=3, Ncn=3, PSDPupdate=0.5, PL2full=0.1;
- for HIP: IndTufa=1, PT1mn=1, PT1rrvs=0.5, PT1cn=0.9, PT2rrvs=1, Phipmncn=1, Phipufacn=1, PSDPupdate=0.5, PL2full=0.1

The results show that on average HIP (2.1) scenario is also accepted. We supposed that in 50% of the cases, SIP sessions are handed off without the need for SDP update. Due to this PSDPupdate probability, the average service interruption time is below 250 ms, hence we accept the alternative. However care must be taken, because in the events of SDP update needed, HIP (2.1) will not fulfil the service interruption delay requirement. HIP (2.1) performs much worse than the other alternatives regarding other performance aspects, such as the HO related message overhead, and the session establishment related message overhead.

For PMIP (2.1), the average service interruption delay is still higher than 250 ms. By the analysis of Table 5 (first part, 4th column), we can deduce that the number of messages on the other network parts already cause a very high real-time service interruption delay. Hence the average service interruption delay, assuming PSDPupdate=0.5, remains still above 250 ms.

6.5.1 Sensitivity of the terminal scores to the network delay between the MN and the UFA_GW

Figure 46 illustrates the sensitivity of terminal scores of the alternatives to the one-way average transmission delay of network part (I/VII), between the MN and its UFA_GWs. The three subfigures illustrate how the terminals scores of the alternatives are changing under the “Objective” (i.e., under all criteria), under the “performance” criteria, and under the “service interruption delay” criterion. If the service interruption delay of an alternative gets higher than the maximum hard constraint \( P_{\text{max}}=250 \text{ms} \), the alternative fails, and is assigned with zero terminal score regarding this criterion and the parent criteria of that child criterion. Our performance category assignment function gives \( v=7 \), i.e., the best score, to alternatives performing between 0 and 190 ms. Then the performance category value is decreasing to 0 using a geometrical scale of Type-3, within the range 190 ms and 250 ms. This means that from 0 to \(~200\) ms, we do not differentiate the alternatives, all are considered equally good.

The subfigures show that the alternatives have a constant terminal score from 0 until a given delay. This is the range where the service interruption delay is below \(~200\) ms. Then, with the increase of the access network delay, the alternatives continuously get into worse and worse performance categories. It can be seen that the PMIP application scenarios (2.1 and 2.3) get worse sooner than the HIP application scenarios (1.1 and 1.3).

HIP (2.1) fails the hard constraint already when the one-way link delay between the MN and the UFA_GW/L2 PoA is less than 5 ms. PMIP (2.2) fails even at 0 link delay (the delays at the other network parts already exceed the hard constraint for service interruption delay). The PMIP alternatives (1.2 and 3.2) seem to fulfill the 200 ms criterion until 30 ms, and reach 250 ms service interruption delay between 50 and 55 ms of one-way transmission delay on network part I and VII. The HIP alternatives seem to work fine until 50-55 ms and are rejected between 65 and 75 ms of access network delay.
One-way delay of the network part bw. MN and UFA_GW [ms] (CNs are MNs).

Terminal scores of the alternatives under all criteria.
Figure 46: Sensitivity of the ranking of alternatives to the one-way delay between the MNs and their serving UFA_GWs (CNs are also MNs).
One-way delay of the network part bw. MN and UFA_GW [ms] (CNs are servers).
6.5.2 Sensitivity of the terminal scores to the weights of the main criteria

In this section we present the sensitivity of the rankings of the alternatives to the variation of the weights of the main criteria, i.e., the performance, security and deployment criteria, under fixed network parameters given in Table 2. For all evaluations, while the weight $c_i$ of the perturbed criterion is increased from zero to one, the weights of the other three main criteria are decreased in a proportional way, so that the sum of the main criteria weights is one. The differences between the gradients of the curves show that how the importance of a criterion (and the proportionally decreasing importance of the other main criteria) do influence the judgment of an alternative.

In Figure 48, we can observe that as the performance criterion becomes the only important criterion, the alternatives HIP (1.1 and 3.1), and PMIP (1.2 and 3.2) approach to each other. Under the fixed network parameters given in Table 2, and having the basic assumptions that the different probabilities and number of peers triggering signalling events are set to 1 (e.g., PL2full=1, Ncn=1, Ncandidates=1 etc), we can observe that the alternatives have almost the same performance costs. Naturally, HIP (2.1) and PMIP (2.2) fail due to their too high service interruption delay.

In Figure 49, as the security becomes more important, the difference between HIP and PMIP based signalling schemes increase, due to the difference in the built-in, tunable DoS resistance function of HIP compared to the simple cookie-based solution of IKEv2.

Figure 50 illustrates the same phenomenon for the deployment criterion, i.e., with increasing importance the HIP alternative becomes better. However, note that the deployment cost is measured in a simplified manner. It is measured with the number of surplus modules needed above TCP/IP stack in different UFA entities. HIP is better because it provides an integrated solution for handling security control and mobility. The PMIP based scheme requires IKEv2 and PMIP modules for the same functionality.
Figure 48: Terminal scores of the alternatives under perturbed criteria weights, in function of the performance criterion weight.
Figure 49: Terminal scores of the alternatives under perturbed criteria weights, in function of the security criterion weight.
Figure 50: Terminal scores of the alternatives under perturbed criteria weights, in function of the deployment criterion weight.
6.6 Discussion of the results

Within the constraints of this evaluation:

- Under the jointly specified criteria and criteria weights (Annex F),
- Assuming a network model with slightly overestimated delay parameters at different parts for having the worst case scenarios (Table 2),
- Endeavouring to define performance categorization scales and criteria measurement metrics which reflect standard requirements or our objective judgement (Figure 41),
- We have evaluated the combined HIP and PMIP based signalling schemes in two extreme network scenarios, i.e., “CNs are all MNs”, and “CNs are all servers in the core network/ or the Internet”, and
- And in application scenarios, i.e., (1) establishment and handing off non-SIP sessions, (2) establishment and handing off of SIP sessions in the same way as non-SIP sessions, (3) establishment of SIP sessions, and handing them off in a more optimal way performing SDP update before physical handover.

The results show that HIP (2.1) and PMIP (2.2) scenarios could introduce too much service interruption delay hence SIP sessions must update their SDP information proactively before physical handover, as it is performed in (HIP 3.1) and PMIP (3.2) signalling scenarios.

Under the previously mentioned constraints and simplifications, the HIP based alternative seems to behave slightly better than the PMIP based alternative. However, this is due to the better DoS resistance built-in into HIP, protecting UFA_GWs, and the highly integrated mobility and security control functionalities in the combined HIP based signalling scheme. Note that the proposed HIP module still needs detailed design, development and testing to realize the HIP delegation service functionalities.
7 Conclusion

With the explosive proliferation of mobile communications and wireless computing devices, the scalability property is becoming an increasingly important feature of wireless communication in pervasive networking scenarios, because of its impact on user’s quality of experience. At the same time operators wish to improve the control over their networks with regard to resources and mobility with the proliferation of real time, high bitrate, data intensive mobile access services.

Eurescom study P1857 has designed and proposed a disruptive architecture named Ultra Flat Architecture (UFA) that overcomes the scalability issues by optimizing service establishment and mobility management. Based on UFA, a flat and fully distributed architecture, two integrated protocol scenarios has been defined:

- 802.21 in combination with HIP and SIP,
- 802.21 in combination with PMIP and SIP.

The study has provided a description of the UFA_GW architecture for the implementation of the two integrated protocol scenarios:

- Description of UFA nodes (UFA_GW, UFA Core Node),
- Description of the functional modules in the UFA_GW,
- Macro definition of the two integrated scenarios,
- The terminal attachment procedures, including AAA, security and IP addressing,
- The session establishment, maintenance and QoS procedures,
- The mobility procedures, including:
  - Media independent handover by using 802.21 framework,
  - End-to-end mobility solutions (i.e., SIP, new delegation-based HIP), and a hierarchical mobility solution (i.e., PMIP),
  - Context transfer between source base station and target base station based on Context Transfer Protocol (CXTP).

The comparison of the integrated protocol scenarios has been made according to the kind of applications launched by the MN to CNs, SIP applications and non-SIP applications. We differentiate when CNs are other MNs or when MNs are servers. We divided the comparison in three main usecases:

1) For non-SIP applications, comparison of the HIP and the PMIP procedures based on UFA signalling schemes,

2) For SIP-applications, we consider and evaluate when mobility execution for SIP applications and non-SIP applications are managed by HIP or PMIP makes the handover (in the same way as for 1), furthermore after physical handover SIP may update the SDP (QoS) of the SIP session. SIP re-INVITE procedures have to be added after HO completion of HIP or PMIP, in order to update SDP according to the resources on the T_UFA_GW / candidate L2 PoA.

3) For SIP applications, we consider and evaluate slightly different handover procedures from usecase 2). Now the SIP re-INVITE procedure might replace 802.21 MIH_Net_HO_commit exchange to the MN in order to detach from the S_UFA_GW and attach to the T_UFA_GW. SDP update may be performed before the physical handover thanks to the SIP mobility (re-INVITE) procedure. Otherwise, the HIP and PMIP procedures remain the same.

The results show that HIP and PMIP scenarios when we consider SIP applications could introduce too much service interruption delay hence SIP sessions must update their SDP information proactively before physical handover, as it is performed in the usecase 2) when mobility execution of SIP applications is performed by HIP and PMIP signalling scenarios.

Under the previously mentioned constraints and simplifications, the HIP based alternative seems to behave slightly better than the PMIP based alternative. However, this is due to the better DoS resistance built-in into HIP, protecting UFA_GWs, and the highly integrated mobility and security control functionalities in the combined HIP based signalling scheme. Note that the proposed HIP
module still needs detailed design, development and testing to realize the HIP delegation service functionalities.

The Eurescom P1857 study has proved that a flat and fully distributed architecture, with customize protocols scenarios could provide a solution to the scalability issue of mobile and convergent network. The results of the study will be used as background for a CELTIC project named MEVICO. A new collaborative project under the EC will be prepared in 2011, for a possible submission early 2012.
Annex A  Registration/authentication procedures defined in 3GPP standards

This phase aims at checking and preparing the user access to Access Network and IMS services. It involves different steps among them. As Access Network and IMS are independent and IMS services are considered to be supplementary to those of Access Network, registration / authentication is performed to both of Access Network and IMS levels.

In each level, authentication is performed during registration and is accompanied by credential keys building useful to protect data messages or IMS signalling.

In the following we give the different steps involved in this phase. Figure 51 shows also these steps, detailed messages per step are only given for ATH_5 (Figure 52).

**Figure 51. Registration / authentication procedure to access network and IMS as defined in the standard**

**ATH_1: Registration / authentication to Access Network**

During this step the MN informs the Access Network about its location, the MN and Access Network are mutually authenticated, and user access authorisation is checked. Also security keys are built to be used to ensure the integrity and confidentiality for user data.

Depending on the Access Network, this step is performed either using an Access Network specific layer (e.g. the layer session management of UMTS [4]), or EAP (e.g I-WLAN [1], WiMAX [5]).

For UMTS, I-WLAN [4] and EPS [6], AKA [2] is the authentication method (similar to IMS AKA described in ATH_5 step) and the user access identifier is the IMSI.
In some cases (e.g. I-WLAN), to perform registration/authentication, the MN needs to get the IP address of the first IP router (PDG for I-WLAN). The registration/authentication to I-WLAN results in the establishment of an IPSEC tunnel between the MN and the PDG.

**ATH_2: Bearer establishment for SIP signalling**

During this step, a bearer is established between the MN and the first IP router in the Access Network for SIP signalling exchanged between MN and P-CSCF beginning from ATH_5.

**ATH_3: IP address acquisition**

The MN asks for an IP address (@IP1) and configures itself with this address. Depending on the Access Network and on the MN configuration, different means for IP address acquisition are possible:

- During bearer establishment for SIP signalling (ATH_2): in this case the signalling used for ATH_2 enables also to vehicle the IP address for MN. This is possible in UMTS [4]. UMTS also enables the next means of IP address allocation.
- Using DHCP (v4 or v6): in this case the DHCP server is located with the IP first router or in an external entity and the IP first router acts a DHCP relay.
- Using stateless IPv6 configuration: stateless IPv6 configuration does not require additional elements in the network (e.g. DHCP server) for IP address allocation. It supposes that the router to which the MN is attached diffuses Router Advertisement containing the IP subnet information. The MN uses the received subnet information to configure its IP layer and build an IP address.

**ATH_4: P-CSCF discovery**

The MN asks for P-CSCF IP address which is useful for the ATH_5 step. Depending on the Access Network and on the MN configuration, different means for P-CSCF discovery are possible [7],[8]:

- During bearer establishment for SIP (ATH_2): in this case the signalling used for ATH_2 enables also to vehicle the P-CSCF IP address. This is possible in UMTS. UMTS also enables the next means for P-CSCF discovery.
- Using DHCP directly or DHCP with DNS (RFC[2131], RFC[3361], RFC[2132], RFC[3263]).
- Using configuration information already available in the MN.

**ATH_5: Registration / authentication to IMS**

IMS registration and authentication are coupled (Figure 52). Registration messages are used to authenticate the user in a way that the user is registered only when it is authenticated. The MN initiates this procedure by sending a SIP REGISTER request to its home network through the P-CSCF identified in ATH 4. As there could be many S-CSCF within a home network, an appropriate S-CSCF responsible of the MN is selected by the I-CSCF and the HSS. During this procedure, the **IP route for SIP signalling** between MN and S-CSCF is thus discovered through SIP headers (see appendix A) and memorised in MN and S-CSCF based on MN IP address (@IP1), P-CSCF IP address (@P-CSCF), S-CSCF IP address (@S-CSCF).

These routes enable subsequent SIP requests (e.g. INVITE) to follow these discovered routes. Authentication procedure is performed based on user identities and is accompanied by building a Security Association (SA) between MN and P-CSCF for the integrity and confidentiality protection of SIP messages. Practically and according to the 3GPP standard, IPSEC is thought as the best mean to build this SA.

User identities are: the private identity (IMPI) which uniquely identifies the user subscription and the public identity (IMPU) which represents the user SIP URI or tel URI to be registered (identities used to used for requesting communication with other users).
As the IMS is defined within 3GPP and given the fact that historically the IMS has been defined for UMTS, the standard [25] specifies an IMS authentication mechanism similar to the one specified for accessing UMTS services and called Authentication and Key Agreement (AKA) [2]. The only difference between UMTS AKA procedure and IMS AKA procedure is related to the protocol used to transport security parameters (UMTS specific protocols for UMTS and SIP for IMS) and to the user identity used for authentication (IMSI for UMTS and IMPI for IMS).

IMS AKA achieves mutual authentication between a specific module within the terminal (IP multimedia Services Identity Module, ISIM) and the HSS; both of them storing shared information (long term security key, a shared sequence number and the user private and public identities (IMPI, IMPU)). IMS AKA is a challenge response protocol where the S-CSCF challenges the terminal. If the terminal returns the response expected by the S-CSCF it is authenticated. IMS AKA is mandated for all access systems (3GPP, 3GPP2, fixed broadband accesses); however when terminals do not support ISIM the standard specifies other authentication mechanisms.

Detailed message flow for ATH_5 is provided in Figure 52:

![Figure 52. ATH_5. Registration/authentication to IMS](image)

- The terminal sends to the IMS an initial REGISTER request containing its private identity (IMPI) and its public identity (IMPU).
- Based on the received user private identity, the S-CSCF downloads from the HSS a quintet containing a challenge. The quintet does not include the shared secret but does include information derived from this shared key (a random challenge (RAND), the expected result
(XRES), the network authentication token (AUTN), the integrity Key (IK) and the ciphering key (CK)).

- In order to authenticate the user private identity (IMPI), the S-CSCF rejects the initial REGISTER request by sending a SIP UNAUTHORIZED response containing the quintet information except XRES.

- The P-CSCF removes the CK, the IK and forwards the message to the terminal.

- The terminal checks if the received AUTN corresponds to the one calculated based on the secret key and the sequence number, and if yes the network is authenticated. The terminal then calculates the RES, CK and IK based on the shared key and the received RAND. It then sends a second REGISTER request containing its private user identity, its public identity, and RES.

- The P-CSCF forwards the received message to the S-CSCF which authenticates the user if RES is equal to XRES. It informs the HSS that the user is now registered and the HSS stores the S-CSCF address to which MN is registered.

- The S-CSCF sends OK message to the MN via the P-CSCF.

During SIP message exchanges for registration/authentication procedure, the PCSCF and the MN meet through dedicated SIP headers on the IP addresses, transport ports, integrity and encryption algorithms that will be used for the IPSEC tunnel. These elements as well as the IK and CK are used by MN and CN to build locally the IPSEC SA for integrity and confidentiality protection of SIP messages within the IPSEC. No further messages are thus needed (e.g. IKE v2) apart from those given in Figure 52 for IPSEC SA building.

The registration / authentication to IMS procedure leads to set different user related contexts in the IMS and MN elements as shown in Figure 51.

- In the MN: User identities (IMPI, IMPU), @IP1, IP route for SIP signalling to S-CSCF (@IP1, @P-CSCF, @S-CSCF), IPsec SA.

- In the P-CSCF: User identities, @IP1, IP route for SIP signalling to S-CSCF (@IP1, @P-CSCF, @S-CSCF), IP route for SIP signalling to MN (@S-CSCF, @P-CSCF, @IP1), IPsec SA.

- In the S-CSCF: User identities, @IP1, IP route for SIP signalling to S-CSCF (@IP1, @P-CSCF, @S-CSCF), IP route for SIP signalling to MN (@S-CSCF, @P-CSCF, @IP1), user profile downloaded from the HSS.

- In the HSS: user profile, user registered in S-CSCF.

The IPsec SA is defined with two databases as described in Annex D.

ATH_5 supposes two rounds of Register / OK messages in order to authenticate the user. At the end of ATH_5 an IPSEC tunnel is build between the MN and the P-CSCF. The first round is aimed to challenge the user and check its identity.

It is also proposed for this classical ATH_5, in [3] (Annex T), to perform a single round of SIP REGISTER / 200 OK. The user will be authenticated based on:

- A binding in the HSS between its IMS identities (IMPI, IMPU) and Access Network identity (IMSI) on one side;

- A binding in the HSS between Access Network identity (IMSI) and the IP address acquired by the MN in ATH_1 or in ATH_3.

It is the S-CSCF when receiving the SIP REGISTER from the MN including the user IP address and user IMS identity (IMPI) that asks the HSS to forward him the IP address mapped to IMSI – IMPI, IMPU. If this address is the one received in the SIP REGISTER then the user is authenticated.

The disadvantage of this method is that there is no mean to build the IPSEC tunnel between the MN and P-CSCF, since the user is not challenged and there is no CK and IK keys transferred to the P-CSCF.
Annex B  EAP-AKA authentication defined in 3GPP standards for non-3GPP access networks

Among the EAP methods, the EAP-AKA is the most powerful and widespread authentication method for network access authorization to non-3GPP access networks [23]. This method reuses the 3G AKA procedure network elements, but modifies the transport messages and the generation of session keys.

Already the L2 authentication process needs to send messages to the core network, in order to authenticate both the user and the network. A design goal of the UFA architecture is to optimize the number of message exchanges to the UFA core nodes, i.e., the AAA server and HSS. Section 4.3 shows on the example of the EAP-AKA procedure, how to integrate L2 and upper layer (i.e., HIP-level) access authorization. We propose a cross-layer commitment scheme among the MN, the L2 PoA, and the serving UFA_GW, to cease HIP-level network authentication message exchanges to the UFA core nodes. Note, that the proposed commitment scheme can also be applied for EAP-SIM, 3G AKA, 2G SIM-based and other authentication methods, where upper layer access authorization is needed beyond the L2 network access authorization.

Figure 53. EAP-AKA authentication procedure depicts the standardized EAP-AKA authentication procedure used for non-3GPP access networks, such as I-WLAN. The network elements in the figure can be generalized in the following way for the UFA. WLAN UE and USIM are the MN. WLAN AN represents the L2 PoA together with the access network. The 3GPP AAA server and the HSS are UFA core nodes.

1. A connection is established between the WLAN UE and the WLAN AN, using a Wireless LAN technology specific procedure (out of scope for this specification).
2. The WLAN AN sends an EAP Request/Identity to the WLAN UE. EAP packets are transported over the Wireless LAN interface encapsulated within a Wireless LAN technology specific protocol.
3. The WLAN UE sends an EAP Response/Identity message. The WLAN UE sends its identity complying with Network Access Identifier (NAI) format specified in 3GPP TS 23.003. NAI contains either a pseudonym allocated to the WLAN UE in previous authentication or, in the case of first authentication, the IMSI.
4. The message is routed towards the proper 3GPP AAA Server based on the realm part of the NAI. The routing path may include one or several AAA proxies (not shown in the figure).
5. The 3GPP AAA Server receives the EAP Response/Identity packet that contains the
subscriber identity. The identifier of the WLAN radio network, VPLMN Identity and the MAC address of the WLAN UE shall also be received by the 3GPP AAA Server in the same message.

6. 3GPP AAA Server identifies the subscriber as a candidate for authentication with EAP-AKA, based on the received identity. The 3GPP AAA Server then checks that it has an unused authentication vector available for that subscriber. If not, a set of new authentication vectors is retrieved from HSS/HLR. A mapping from the temporary identifier to the IMSI may be required. In addition, 3GPP AAA Server shall retrieve authentication vectors from HLR/HSS when it detects that the VPLMN selected by a user has changed. This can happen, for example, when a user is performing a VPLMN re-selection procedure and is initiating a new authentication procedure via a new VPLMN. The HSS/HLR shall check if there is a 3GPP AAA Server already registered to serve for this subscriber. In case the HSS/HLR detects that another 3GPP AAA Server has already registered for this subscriber, it shall provide the current 3GPP AAA Server with the previously registered 3GPP AAA Server address. The authentication signaling is then routed to the previously registered 3GPP AAA Server with Diameter-specific mechanisms, e.g., the current 3GPP AAA Server transfers the previously registered 3GPP AAA Server address to the AAA proxy or the WLAN AN, or the current 3GPP AAA Server acts as a AAA proxy and forwards the authentication message to the previously registered 3GPP AAA Server. It could also be the case that the 3GPP AAA Server first obtains an unused authentication vector for the subscriber and, based on the type of authenticator vector received (i.e. if a UMTS authentication vector is received), it regards the subscriber as a candidate for authentication with EAP-AKA.

7. The 3GPP AAA Server requests again the user identity, using the EAP Request/AKA Identity message. This identity request is performed as the intermediate nodes may have changed or replaced the user identity received in the EAP Response Identity message, as specified in ref. [24]. However, this new request of the user identity can be omitted by the home operator if there exist the certainty that the user identity could not be changed or modifies by any means in the EAP Response Identity message.

8. The WLAN AN forwards the EAP Request/AKA Identity message to the WLAN UE.

9. The WLAN UE responds with an identity that depends on the parameters contained in the EAP Request/AKA Identity message; for details cf. TS 24.234 [47].

10. The WLAN AN forwards the EAP Response/AKA Identity to the 3GPP AAA Server. The identity received in this message will be used by the 3GPP AAA Server in the rest of the authentication process. If an inconsistency is found between the identities received in the two messages (EAP Response Identity and EAP Response/AKA Identity) so that the user profile and authentication vectors previously retrieved from HSS/HLR are not valid, these data shall be requested again to HSS/HLR (step 6 shall be repeated before continuing with step 11). In order to optimize performance, the identity re-request process (the latter four steps) should be performed when the 3GPP AAA Server has enough information to identify the user as an EAP-AKA user, and before user profile and authentication vectors retrieval, although protocol design in Wx interface may not allow to perform these four steps until the whole user profile has been downloaded to the 3GPP AAA Server.

11. 3GPP AAA Server checks that it has the WLAN access profile of the subscriber available. If not, the profile is retrieved from HSS. 3GPP AAA Server verifies that the subscriber is authorized to use the WLAN service. Although this step is presented after step 6 in this example, it could be performed at some other point, however before step 14.

12. New keying material is derived from IK and CK, cf 0. This keying material is required by EAP-AKA, and some extra keying material may also be generated for WLAN technology specific confidentiality and/or integrity protection. A new pseudonym and/or re-authentication ID may be chosen and protected (i.e. encrypted and integrity protected) using EAP-AKA generated keying material.

13. 3GPP AAA Server sends RAND, AUTN, a message authentication code (MAC) and two user identities (if they are generated): protected pseudonym and/or protected re-authentication id to WLAN AN in EAP Request/AKA-Challenge message. The sending of the re-authentication id depends on 3GPP operator's policies on whether to allow fast re-authentication processes or
not. It implies that, at any time, the 3GPP AAA Server decides (based on policies set by the operator) to include the re-authentication id or not, thus allowing or disallowing the triggering of the fast re-authentication process. The 3GPP AAA Server may send as well a result indication to the WLAN UE, in order to indicate that it wishes to protect the success result message at the end of the process (if the outcome is successful). The protection of result messages depends on home operator’s policies.

14. The WLAN AN sends the EAP Request/AA-Challenge message to the WLAN UE.
15. The WLAN UE runs UMTS algorithm on the USIM. The USIM verifies that AUTN is correct and hereby authenticates the network. If AUTN is incorrect, the terminal rejects the authentication (not shown in this example). If the sequence number is out of synch, terminal initiates a synchronization procedure, c.f. [4]. If AUTN is correct, the USIM computes RES, IK and CK. The WLAN UE derives required additional new keying material from the new computed IK and CK from the USIM, checks the received MAC with the new derived keying material. If a protected pseudonym and/or re-authentication identity were received, then the WLAN UE stores the temporary identity(s) for future authentications.

16. The WLAN UE calculates a new MAC value covering the EAP message with the new keying material. WLAN UE sends EAP Response/AA-Challenge containing calculated RES and the new calculated MAC value to WLAN AN. The WLAN UE shall indicate if it received the same indication from the 3GPP AAA Server. Otherwise, the WLAN UE shall omit this indication.
17. WLAN AN sends the EAP Response/AA-Challenge packet to 3GPP AAA Server
18. The 3GPP AAA Server checks the received MAC and compares XRES to the received RES.
19. If all checks in step 18 are successful, the 3GPP AAA Server shall send the message EAP Request/AA-Notification, previous to the EAP Success message, if the 3GPP AAA Server requested previously to use protected successful result indications. This message is MAC protected.
20. The WLAN AN forwards the message to the WLAN UE.
21. The WLAN UE sends the EAP Response/AA-Notification.
22. The WLAN AN forwards the EAP Response/AA-Notification message to the 3GPP AAA Server. The 3GPP AAA Server shall ignore the contents of this message
23. The 3GPP AAA Server sends the EAP Success message to WLAN AN (perhaps preceded by an EAP Notification, as explained in step 20). If some extra keying material was generated for WLAN technology specific confidentiality and/or integrity protection then the 3GPP AAA Server includes this keying material in the underlying AAA protocol message (i.e. not at the EAP level). The WLAN AN stores the keying material to be used in communication with the authenticated WLAN UE.
24. The WLAN AN informs the WLAN UE about the successful authentication with the EAP Success message. Now the EAP AKA exchange has been successfully completed, and the WLAN UE and the WLAN AN share keying material derived during that exchange.
25. If there is no other ongoing WLAN Access session for the subscriber detected by the 3GPP AAA Server, and the WLAN registration for this subscriber is not performed previously, then the 3GPP AAA Server shall initiate the WLAN registration to the HSS/HLR. Otherwise, the 3GPP AAA Server shall compare the MAC address, VPLMN Identity and the WLAN access network information of the authentication exchange with the same information of the ongoing sessions. If the information is the same as with an ongoing session, then the authentication exchange is related to the ongoing session, so there is no need to do anything for old sessions. If it is the same subscriber but with a different MAC address, or with a different VPLMN identity or with different radio network information that is received in any ongoing session, the 3GPP AAA Server then considers that the authentication exchange is related to a new WLAN Access session. It shall terminate an old WLAN Access session after the successful authentication of the new WLAN Access session, based on the policy whether simultaneous sessions are not allowed, or whether the number of allowed sessions has been exceeded. When the MAC addresses (the old one and the new one) are equal and the WLAN radio network information received is different from the old one, it is up to home operator local policies to interpret this fact as a fraud or a legal situation, and then proceed either
deleting the old session or allowing both (the old and the new one)

The authentication process may fail at any moment, for example because of unsuccessful checking of MACs or no response from the WLAN UE after a network request. In that case, the EAP AKA process will be terminated as specified in ref [24] and an indication shall be sent to HSS/HLR.
Annex C  IP address allocation in 3GPP standards for non-3GPP access networks

IP address allocation in 3GPP Relase 9, Wifi and WiMax networks is described in [1]. When using WLAN Direct IP Access, a WLAN UE needs to use its local IP address only. When using WLAN 3GPP IP Access, a WLAN UE shall use two IP addresses; its local IP address and remote IP address.

WLAN UE's local IP address identifies the WLAN UE in the WLAN AN. In systems supporting only WLAN Direct IP Access, the WLAN UE's local IP address is assigned by the WLAN AN; in a WLAN 3GPP IP Access enabled system, it can be assigned by a WLAN or by a PLMN (a VPLMN in roaming case and a HPLMN in non-roaming case). For the WLAN-assigned local IP address, which belongs to the address space of WLAN AN, there is no additional requirement on the WLAN. WLAN UE's local IP address allocation by the PLMN is for further study.

When using WLAN 3GPP IP Access, a WLAN UE's remote IP address identifies the WLAN UE in the network that the WLAN UE is accessing for the 3G PS service. It shall be used for the inner packet of the WLAN UE-initiated tunnel. It can be assigned by HPLMN, VPLMN or an external IP network. The remote IP address can be statically or dynamically assigned. The only case where VPLMN assigns the remote IP address for the WLAN UE is when the WLAN UE-initiated tunnel terminates at the VPLMN's PDG. When the WLAN UE's remote IP address is allocated by the external IP network, the PDG is required to have an interface with an address allocation server, such as AAA or DHCP, belonging to the external IP network. For the WLAN UE's remote IP address, IPv4 addresses shall be supported. When the WLAN UE accesses 3G PS based services using an IPv6 network such as IMS services, IPv6 addresses shall be supported for the WLAN UE's remote IP address. To avoid any clashes between addresses used in WLAN AN and PLMN and to enable correct routing of packets sent out by the WLAN UE the PLMN operator should allocate public addresses to network nodes, which are addressed by WLAN UEs.

When a WLAN UE accesses several 3G PS based services with different W-APNs simultaneously, the WLAN UE can get several remote IP addresses. There may be several WLAN UE-initiated tunnels for the services.

**Static and Dynamic Remote IP Address**

Remote IP address can be allocated to a WLAN UE in four different ways:

- The HPLMN operator assigns a Remote IP address permanently to the WLAN UE (static remote IP address).
- The HPLMN operator assigns a Remote IP address to the WLAN UE when the tunnel is established to the PDG in the home network (dynamic HPLMN remote IP address).
- The VPLMN operator assigns a Remote IP address to the WLAN UE when the tunnel is established to the PDG in the visited network (dynamic VPLMN remote IP address).
- The external IP network operator assigns a permanent or dynamic Remote IP address to the WLAN UE (external Remote IP address allocation).

It is the HPLMN operator that defines in the subscription whether static IP address allocation is used. When static IP address allocation is used, a WLAN UE either can include its static IP address in the tunnel setup request message, or indicate in the tunnel setup request message that the network should configure the static IP address of the WLAN UE or the network simply provides the static address to the WLAN UE.

In UFA, the serving UFA_GW is a DHCP server or relay, and the L2 PoA is a bridge. IP address allocation for MNs could be done during the L2 authentication procedure, within EAP messages,
however this is not specified in standards. Currently DHCPv6 protocol is the most common configuration provisioning protocol, which is used for address allocation among other tasks as described in [25].

A router attached to a network will announce it as a router sending periodic Router Advertisements (RA's). If the router wishes that the attached clients have to use DHCPv6 for acquiring an IPv6 address, then it can signal that with setting the 'O' and 'M' bits in the Router Advertisement (RA). The two bits of importance within a Router Advertisement (RA) are:

a. M-bit: 1-bit "Managed address configuration" flag. When set, clients use DHCPv6 protocol for address configuration.

b. O-bit: 1-bit "Other stateful configuration" flag. When set, hosts use DHCPv6 to obtain 'other' (non-address) information.

On a client enabled with the DHCPv6 stack, the DHCP procedure is typically initiated when either the client receives a notification from the attached router to run DHCPv6 (by the 'O' and 'M' bits in the Router Advertisement (RA)), or if the client detects no directly connected routers. However, there's nothing to prohibit DHCPv6 to run always; it is just that it SHOULD be run if M or O bits are set.

A directly connected DHCPv6 server or relay will reply to the request from the DHCPv6 client.
Annex D  IPsec Tunnel context

In IPsec terminology, the outbound traffic is the traffic that need to be protected by IPsec and the Inbound traffic is the traffic that needs IPSec decapsulation. A security association is identified uniquely using the Security Parameter Index (SPI) contained within IPsec databases and IPsec header. Entities implementing IPsec use two main contexts / databases:

1) The Security Policy Database (SPD) maintains the list of security policies (service) to apply to inbound / outbound traffic. It is consulted during the processing of all inbound or outbound traffic and contains:
   - Traffic selectors that identify the packets to which a security policy shall be applied. They are the IP source address, the destination IP address, the source port, the destination port and the next layer of the received packets.
   - The security policies which are:
     o For outbound traffic:
       ▪ Protect, bypass or discard the traffic.
       ▪ If protect and a SA is not created for that traffic then it shall be created. Else, if the SA is created, a link to the Security Association Database (SAD) is provided.
       ▪ IPsec mode (tunnel/transport) for SA to be created, if tunnel mode: local/remote tunnel address.
       ▪ AH/ESP algorithms for SA to be created.
     o For inbound traffic: the way to search the related Security association (SA) in the SAD (Based on SPI, or based on SPI and remote IP@)

2) The Security Association Database (SAD) contains the description of SA created for inbound and outbound traffic. This description indicates how to process the traffic:
   - For outbound it contains: AH/ESP algorithms/keys, IPsec mode, tunnel header
   - For inbound contains: SPI, AH/ESP algorithms/keys, IPsec mode, tunnel header, and selectors. After applying the AH and ESP algorithms as specified in the SAD, the obtained packet shall be compared to the selectors identified by the SAD. If they do not match, the packet shall be discarded.
Annex E  L2 fast re-authentication techniques

This section gives some examples for L2 fast re-authentication methods that were studied by 802.11 security workgroup in [22]. Part of the methods is access technology dependent. This study did not aim to analyze in details L2 re-authentication methods. We suppose in this study, that the transport of EAP methods is supported over the L2 control protocol.

E.1 Access technology dependent L2 fast re-authentication techniques

IEEE 802.11i

- MN gets MIH_Net_Commit request from the UFA_CL of the S_UFA_GW
- MN, target L2 PoA, and the AAA server run a 802.11i based authentication through the source L2 PoA.
- The MN sends MIH_Net_HO_commit response to the UFA_CL of the S_UFA_GW

IEEE 802.11r fast BSS transition

- MN knows that the target L2 PoA and the source L2 PoA support 802.11r Fast BSS transition
- After Link_Up indication the MN initiates a fast BSS transition between the MN, the source L2 PoA and the target L2 PoA.

IEEE 802.16e

- The MN gets MIH_Net_Commit request from the UFA_CL of the S_UFA_GW.
- The MN sends to the source L2 PoA a L2 HO indication using L2 PoA as target.
- The source L2 PoA sends to the target L2 PoA MS info and connection context (handover TEKs, associated counters, negotiated capabilities, CID update, etc.)
- MN attaches to the target L2 PoA with delayed MIH_Link_Actions command
- The MN sends MIH_Net_HO_commit response to the UFA_CL of the S_UFA_GW

E.2 EAP and ERP for L2 handovers

The following L2 fast re-authentication should be used for intra-AAA domain, intra- and inter-technology handovers. This could be used in UFA.

An EAP based authentication method, such as the EAP-AKA or EAP-SIM, extended with support for EAP Re-authentication Protocol (ERP) [21] on L2:

- The MN gets MIH_Net_Commit request from the UFA_CL of the S_UFA_GW.
- The MN initiates proactive ERP reauthentication with the target L2 PoA, the local proxy AAA server, via the source L2 PoA.
- MN answers MIH_Net_HO_commit response.

E.3 Inter-AAA L2 handovers

For inter-AAA domain handover, the following method is recommended. It should be used for handovers between different UFA domains, or from the UFA to other network domains.

- The MN gets MIH_Net_Commit request from the UFA_CL of the S_UFA_GW.
- The MN pre-authenticates with new target L2 PoA, communicating through the source L2 PoA.
- The MN sends MIH_Net_HO_commit response to the UFA_CL of the S_UFA_GW.
Annex F  Criterion weight specification forms

The following Excel worksheets were used for the inputs of criterion weight assignment. The criteria weights were calculated as given in Section 6.2.

**Assign weights to the main criteria. Weights reflect the importance of the criteria!**

Please fill out the yellow cells under your name, based on your subjective opinion.

Philippe should always assign weights to the decision makers, (in orange cells), Zoltan just showed an example for weight assignment. These values reflect the weight of the words of the decision maker.

As an example, look on Zoltan's values, but don't let you influence by these. You can choose any real number that you think best.

<table>
<thead>
<tr>
<th>Importance of decision makers (P_d)</th>
<th>Philippe</th>
<th>Pedro</th>
<th>Zoltán</th>
<th>László</th>
<th>Khadija</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low performance cost</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>High security</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Easy deployment</td>
<td>5</td>
<td>2</td>
<td>8</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Support non-SIP applications</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Calculation method (see attached pdf):**

**A. Direct weight assignment to criteria**

<table>
<thead>
<tr>
<th>p_d</th>
<th>0.428571</th>
<th>0.142857</th>
<th>0.142857</th>
<th>0.142857</th>
<th>0.142857</th>
</tr>
</thead>
<tbody>
<tr>
<td>c_i,d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low performance cost</td>
<td>0.357143</td>
<td>0.5</td>
<td>0.4</td>
<td>0.4</td>
<td>0.375</td>
</tr>
<tr>
<td>High security</td>
<td>0.285714</td>
<td>0.3</td>
<td>0.2</td>
<td>0.4</td>
<td>0.25</td>
</tr>
<tr>
<td>Easy deployment</td>
<td>0.357143</td>
<td>0.2</td>
<td>0.4</td>
<td>0.2</td>
<td>0.375</td>
</tr>
<tr>
<td>Support non-SIP application</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

\[ p_d \times c_{i,d} \]

<table>
<thead>
<tr>
<th>Importance of decision makers (P_d)</th>
<th>Philippe</th>
<th>Pedro</th>
<th>Zoltán</th>
<th>László</th>
<th>Khadija</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low performance cost</td>
<td>0.153061</td>
<td>0.071429</td>
<td>0.057143</td>
<td>0.057143</td>
<td>0.053571</td>
</tr>
<tr>
<td>High security</td>
<td>0.122449</td>
<td>0.042857</td>
<td>0.028571</td>
<td>0.057143</td>
<td>0.035714</td>
</tr>
<tr>
<td>Easy deployment</td>
<td>0.153061</td>
<td>0.028571</td>
<td>0.057143</td>
<td>0.028571</td>
<td>0.053571</td>
</tr>
<tr>
<td>Support non-SIP applications</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Final weights (c_i)**

<table>
<thead>
<tr>
<th>Importance of decision makers (P_d)</th>
<th>Philippe</th>
<th>Pedro</th>
<th>Zoltán</th>
<th>László</th>
<th>Khadija</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low performance cost</td>
<td>0.153061</td>
<td>0.071429</td>
<td>0.057143</td>
<td>0.057143</td>
<td>0.053571</td>
</tr>
<tr>
<td>High security</td>
<td>0.122449</td>
<td>0.042857</td>
<td>0.028571</td>
<td>0.057143</td>
<td>0.035714</td>
</tr>
<tr>
<td>Easy deployment</td>
<td>0.153061</td>
<td>0.028571</td>
<td>0.057143</td>
<td>0.028571</td>
<td>0.053571</td>
</tr>
<tr>
<td>Support non-SIP applications</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Cross-check (must be 1):**

1
In case of more than three criteria, the weight assignment does not always work well, because it is hard to find the good weights. We decided to use pairwise comparison of the criteria, and calculate from the pairwise comparison values the final weights of the criteria.

In the next sheets, you will have to compare the importance of the criteria in column A and B, by replying to the following question:

What is the difference of the importance of criterium A and B? Fill the yellow cells under your name with your subjective difference value between the two criteria.

The accepted values are the following differences:

<table>
<thead>
<tr>
<th>Interpretation</th>
<th>difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>criterium A is as important as criterium B</td>
<td>0</td>
</tr>
<tr>
<td>criterium A is somewhat more important than criterium B</td>
<td>1</td>
</tr>
<tr>
<td>criterium A is more important than criterium B</td>
<td>2</td>
</tr>
<tr>
<td>criterium A is much more important than criterium B</td>
<td>3</td>
</tr>
<tr>
<td>criterium A is vastly more important than criterium B</td>
<td>4</td>
</tr>
<tr>
<td>criterium A is very important compared to criterium B</td>
<td>5</td>
</tr>
<tr>
<td>criterium A is extremely important compared to criterium B</td>
<td>6</td>
</tr>
<tr>
<td>criterium B is somewhat more important than criterium A</td>
<td>-1</td>
</tr>
<tr>
<td>criterium B is more important than criterium A</td>
<td>-2</td>
</tr>
<tr>
<td>criterium B is much more important than criterium A</td>
<td>-3</td>
</tr>
<tr>
<td>criterium B is vastly more important than criterium A</td>
<td>-4</td>
</tr>
<tr>
<td>criterium B is very important compared to criterium A</td>
<td>-5</td>
</tr>
<tr>
<td>criterium B is extremely important compared to criterium A</td>
<td>-6</td>
</tr>
</tbody>
</table>

The difference values you can use are in the 2nd column. Two interpretation of these values are given in the third and fourth column, where Zoltán gave the ratio of the importance of the compared criteria. The difference values assigned by the decision makers can mean different subjective values. That is why everybody should indicate about which importance ratio was he thinking when he assigned difference values (in the last row of the yellow tables). Zoltán used always the (gamma=1) interpretation. The interpretation in the third and fourth column should be referred as gamma=1 and gamma=0.5, respectively.

Assign differences between the performance criteria

<table>
<thead>
<tr>
<th>Importance of decision makers (( P_{d} ))</th>
<th>Philippe</th>
<th>Pedro</th>
<th>Zoltán</th>
<th>László</th>
<th>Khadija</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimize real-time service session interruption delay</td>
<td>Low network attachment procedure overhead</td>
<td>10</td>
<td>5</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>Minimize real-time service session interruption delay</td>
<td>Low session establishment procedure overhead</td>
<td>2</td>
<td>3</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Minimize real-time service session interruption delay</td>
<td>Low handover preparation and execution overhead</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Minimize real-time service session interruption delay (HO)</td>
<td>Minimize handover preparation delay</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>gamma (0.5 or 1)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Calculation method: B. Direct logarithmic difference assignment

Resulting criterium weights

| Minimize real-time service session interruption delay | 0.62 |
| Low network attachment procedure overhead            | 0.0856|
| Low session establishment procedure overhead          | 0.0945|
| Low handover preparation and execution overhead       | 0.0288|
| Minimize handover preparation delay                   | 0.1711|
### Assign differences between security criteria

<table>
<thead>
<tr>
<th>Importance of decision makers ($P_d$)</th>
<th>Philippe</th>
<th>Pedro</th>
<th>Zoltán</th>
<th>László</th>
<th>Khadija</th>
</tr>
</thead>
<tbody>
<tr>
<td>Must support mutual authentication</td>
<td>5</td>
<td>6</td>
<td>8</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>Must protect signaling traffic bw. MN and UFA_GW (yes/no)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Must support mutual authentication</td>
<td>5</td>
<td>6</td>
<td>8</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>Must protect data traffic bw. MN and UFA_GW (yes/no)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Must support mutual authentication</td>
<td>5</td>
<td>6</td>
<td>8</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>May resist DoS from MNs to the UFA_GWs (yes/no)</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Must support mutual authentication</td>
<td>5</td>
<td>6</td>
<td>8</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>May resist MITM attacks (yes/no)</td>
<td>0</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Calculation method:</td>
<td>B. Direct logarithmic difference assignment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Resulting criterion weights ($c_i$)

| $c_i$ | Must support mutual authentication | 0.3224 |
|       | Must protect signaling traffic bw. MN and UFA_GW (yes/no) | 0.2395 |
|       | Must protect data traffic bw. MN and UFA_GW (yes/no) | 0.2169 |
|       | May resist DoS from MNs to the UFA_GWs (yes/no) | 0.1322 |
|       | May resist MITM attacks (yes/no) | 0.0890 |

### Assign differences between easy deployment criteria

<table>
<thead>
<tr>
<th>Importance of decision makers ($P_d$)</th>
<th>Philippe</th>
<th>Pedro</th>
<th>Zoltán</th>
<th>László</th>
<th>Khadija</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low complexity of the MN on signaling plane (number of modules needed)</td>
<td>10</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>Low complexity of the MN on user plane (number of modules needed)</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Low complexity of the UFA_GW on signaling plane (number of modules)</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>Low complexity of the UFA_GW on user plane (number of modules needed)</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Low amount of changes in the IMS core components (number of modules needed)</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Calculation method:</td>
<td>B. Direct logarithmic difference assignment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Resulting criterion weights ($c_i$)

| $c_i$ | Low complexity of the MN on signaling plane (number of modules needed) | 0.5802 |
|       | Low complexity of the MN on user plane (number of modules needed) | 0.3256 |
|       | Low complexity of the UFA_GW on signaling plane (number of modules) | 0.0228 |
|       | Low complexity of the UFA_GW on user plane (number of modules needed) | 0.0256 |
|       | Low amount of changes in the UFA core components (number of modules needed) | 0.0457 |
Finally, we need to determine the weights (importances) of high message overheads in different network parts. The same method is used, as in case of the sub criteria worksheet, i.e., subjective difference assignment must be done between each pair of criteria.

Assess subjective preference differences between the importance of the message overhead on different network parts specified in Column A and Column B

<table>
<thead>
<tr>
<th>Importance of decision makers (P_d)</th>
<th>Philippe</th>
<th>Pedro</th>
<th>Zoltán</th>
<th>László</th>
<th>Khadija</th>
</tr>
</thead>
<tbody>
<tr>
<td>Between MN &amp; UFA_GW (wireless interface included)</td>
<td>Between UFA_GW and UFA core nodes</td>
<td>15</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Between MN &amp; UFA_GW (wireless interface included)</td>
<td>Between source and target UFA_GWs</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Between MN &amp; UFA_GW (wireless interface included)</td>
<td>Between MN’s UFA_GW and CN’s UFA_GW</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Between MN &amp; UFA_GW (wireless interface included)</td>
<td>Between UFA core nodes</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Between MN &amp; UFA_GW (wireless interface included)</td>
<td>Between UFA core nodes</td>
<td>5</td>
<td>6</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

Calculation method:
B. Direct logarithmic difference assignment

Resulting criterion weights (c_i) for network parts

| Between MN & UFA_GW (wireless interface included) | 0.6117 |
| Between UFA_GW and UFA core nodes | 0.0932 |
| Between source and target UFA_GWs | 0.1688 |
| Between MN’s UFA_GW and CN’s UFA_GW | 0.1029 |
| Between UFA core nodes | 0.0233 |
Annex G  Analysis of the message traces of the procedures

For the evaluation of the combined signalling schemes in different scenarios regarding their performance costs, we analyzed the number of control messages on different parts of our network model caused by the different procedures.

The service interruption delays were calculated using the red messages in the handover procedures. The handover preparation delay was calculated by counting the messages from the MIH_Link_Going_Down message until the physical handover (i.e., until the red messages).

On L2, EAP-AKA based authentication is supposed. In practice this is supported in I-WLAN today.

<table>
<thead>
<tr>
<th>Message name</th>
<th>src</th>
<th>dst</th>
<th>network part</th>
<th>number of messages per inter-UFA_GW handoff</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2 attachment</td>
<td>PoA,MN</td>
<td>MN,PoA</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>EAP Request/Identity</td>
<td>PoA</td>
<td>MN</td>
<td></td>
<td>1 PL2full</td>
</tr>
<tr>
<td>EAP Response/Identity</td>
<td>MN</td>
<td>PoA</td>
<td></td>
<td>1 PL2full</td>
</tr>
<tr>
<td>EAP Request/Identity</td>
<td>PoA</td>
<td>local AAA</td>
<td></td>
<td>3 PL2full</td>
</tr>
<tr>
<td>EAP Response/Identity</td>
<td>local AAA</td>
<td>AAA</td>
<td></td>
<td>2 PL2full</td>
</tr>
<tr>
<td>EAP Request/AKA-Identity</td>
<td>AAA</td>
<td>local AAA</td>
<td></td>
<td>2 PL2full</td>
</tr>
<tr>
<td>EAP Request/AKA-Identity</td>
<td>local AAA</td>
<td>PoA</td>
<td></td>
<td>3 PL2full</td>
</tr>
<tr>
<td>EAP Request/AKA-Identity</td>
<td>PoA</td>
<td>MN</td>
<td></td>
<td>1 PL2full</td>
</tr>
<tr>
<td>EAP Request/AKA-Identity</td>
<td>MN</td>
<td>PoA</td>
<td></td>
<td>1 PL2full</td>
</tr>
<tr>
<td>EAP Request/AKA-Identity</td>
<td>PoA</td>
<td>local AAA</td>
<td></td>
<td>3 PL2full</td>
</tr>
<tr>
<td>EAP Request/AKA-Identity</td>
<td>local AAA</td>
<td>AAA</td>
<td></td>
<td>2 PL2full</td>
</tr>
<tr>
<td>EAP Request/AKA-Notification</td>
<td>AAA</td>
<td>local AAA</td>
<td></td>
<td>2 PL2full</td>
</tr>
<tr>
<td>EAP Request/AKA-Notification</td>
<td>local AAA</td>
<td>PoA</td>
<td></td>
<td>3 PL2full</td>
</tr>
<tr>
<td>EAP Request/AKA-Notification</td>
<td>PoA</td>
<td>MN</td>
<td></td>
<td>1 PL2full</td>
</tr>
<tr>
<td>EAP Request/AKA-Notification</td>
<td>MN</td>
<td>PoA</td>
<td></td>
<td>1 PL2full</td>
</tr>
<tr>
<td>EAP Request/AKA-Notification</td>
<td>PoA</td>
<td>local AAA</td>
<td></td>
<td>3 PL2full</td>
</tr>
<tr>
<td>EAP Request/AKA-Notification</td>
<td>local AAA</td>
<td>AAA</td>
<td></td>
<td>2 PL2full</td>
</tr>
<tr>
<td>EAP Success</td>
<td>AAA</td>
<td>local AAA</td>
<td></td>
<td>2 PL2full</td>
</tr>
<tr>
<td>EAP Success</td>
<td>local AAA</td>
<td>PoA</td>
<td></td>
<td>3 PL2full</td>
</tr>
<tr>
<td>EAP Success</td>
<td>PoA</td>
<td>MN</td>
<td></td>
<td>1 PL2full</td>
</tr>
</tbody>
</table>

L2 re-authentication

<table>
<thead>
<tr>
<th>Message name</th>
<th>src</th>
<th>dst</th>
<th>network part</th>
<th>number of messages per inter-UFA_GW handoff</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP-Initiate/Re-auth</td>
<td>MN</td>
<td>PoA</td>
<td></td>
<td>1 PL2full</td>
</tr>
<tr>
<td>EAP-Initiate/Re-auth</td>
<td>PoA</td>
<td>local AAA</td>
<td></td>
<td>3 PL2full</td>
</tr>
<tr>
<td>EAP-Finish/Re-auth</td>
<td>local AAA</td>
<td>PoA</td>
<td></td>
<td>3 PL2full</td>
</tr>
<tr>
<td>EAP-Finish/Re-auth</td>
<td>PoA</td>
<td>MN</td>
<td></td>
<td>1 PL2full</td>
</tr>
</tbody>
</table>

PL2full: is the probability that full (re-)authentication happens. 1-PL2full is the probability that ERP fast reauthentication is done with a local AAA proxy, that is located in the neighbourhood of the L2 PoAs.

L3 attachment procedures are presented in the followings for HIP and PMIP, respectively. SIP registration happens only when SIP-applications are running. The other messages are always present during attachment.

L3 full re-authentications and fast re-authentications were not considered now. HIP-level fast re-authentications between the MN and the UFA_GW could be performed using HIP UPDATEs (3 messages) on network part 1, and an EAP-Initiate/HIP-auth and EAP-Finish/HIP-auth messages in network part 3. For PMIP, IKEv2 fast re-authentications should be performed with ERP over IKEv2.
<table>
<thead>
<tr>
<th>Message name</th>
<th>src</th>
<th>dst</th>
<th>network part</th>
<th>number of messages per inter-UFA_GW handoff</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPv6 Solicit</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>DHCPv6 Advertise (UFA_GW's IP, HIT)</td>
<td>UFA_GW</td>
<td>MN</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>DHCPv6 Request</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>DHCPv6 Reply (MNs IP)</td>
<td>UFA_GW</td>
<td>MN</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>I1</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>R1</td>
<td>UFA_GW</td>
<td>MN</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>i2</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>EAP-Initiate/HiP-auth</td>
<td>UFA_GW</td>
<td>local AAA</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>EAP-Finish/HiP-auth</td>
<td>local AAA</td>
<td>UFA_GW</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>R2</td>
<td>UFA_GW</td>
<td>MN</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>DHCPv6 Request</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>DHCPv6 Relay-Forward(Request)</td>
<td>UFA_GW</td>
<td>DHCP</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>reply check MN's authorization</td>
<td>DHCP</td>
<td>AAA</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>DHCPv6 Relay-Reply(Reply)</td>
<td>DHCP</td>
<td>UFA_GW</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>DHCPv6 Reply (SIP-related,other central parameters)</td>
<td>UFA_GW</td>
<td>MN</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MIH_Capability_Discover request</td>
<td>UFA_GW</td>
<td>MN</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MIH_Capability_Discover response</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MIH_Register request</td>
<td>UFA_GW</td>
<td>MN</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MIH_Register response</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MIH_Event_Subscribe request</td>
<td>UFA_GW</td>
<td>MN</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MIH_Event_Subscribe response</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>HIP BEX I1</td>
<td>UFA_GW</td>
<td>RVS</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>HIP BEX R1, REG_INFO(RVS)</td>
<td>RVS</td>
<td>UFA_GW</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>HIP BEX R2 Mandated Action Request (REG_REP(MN registered to RVS))</td>
<td>UFA_GW</td>
<td>RVS</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>HIP BEX I2 Mandated Action Reply (REG_REQ(MN to RVS))</td>
<td>RVS</td>
<td>UFA_GW</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>1. Register</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2. Register</td>
<td>UFA_GW</td>
<td>i-CSCF</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3. Cx-Query/Cx-Select-Pull</td>
<td>i-CSCF</td>
<td>HSS</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>4. Cx-Query Resp/Cx-Select-Pull Resp</td>
<td>HSS</td>
<td>i-CSCF</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>5. Register</td>
<td>i-CSCF</td>
<td>S-CSCF</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>6. Cx-Put/Cx-Pull</td>
<td>S-CSCF</td>
<td>HSS</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>7. Cx-Put/Cx-Pull Response</td>
<td>HSS</td>
<td>S-CSCF</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>8. 200 OK</td>
<td>S-CSCF</td>
<td>i-CSCF</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>9. 200 OK</td>
<td>i-CSCF</td>
<td>UFA_GW</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>10. 200 OK</td>
<td>UFA_GW</td>
<td>MN</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>PMIP</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------</td>
<td>--------</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>DHCPv6 Solicit</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>DHCPv6 Advertise (UFA_GW’s IP, HIT)</td>
<td>UFA_GW</td>
<td>MN</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>DHCPv6 Request</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>DHCPv6 Reply (MN’s IP)</td>
<td>UFA_GW</td>
<td>MN</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>IKE_SA_INIT</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>IKE_AUTH</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>EAP-Initiate/Re-auth</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>EAP-Finish/Re-auth</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>IKE_AUTH</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>DHCPv6 Request</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>DHCPv6 Relay-Forward(Request)</td>
<td>UFA_GW</td>
<td>DHCP</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>request check MN’s authorization</td>
<td>DHCP</td>
<td>AAA</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>reply check MN’s authorization</td>
<td>AAA</td>
<td>DHCP</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>DHCPv6 Relay-Reply(Reply)</td>
<td>DHCP</td>
<td>UFA_GW</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>DHCPv6 Reply (SIP-related,other central parameters)</td>
<td>UFA_GW</td>
<td>MN</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MIH_Capability_Discover</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MIH_Capability_Discover</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MIH_Register request</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MIH_Register request</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MIH_Register response</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MIH_Event_Subscribe request</td>
<td>UFA_GW</td>
<td>MN</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MIH_Event_Subscribe request</td>
<td>UFA_GW</td>
<td>MN</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Register</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Register</td>
<td>MN</td>
<td>UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3. Cx-Query/Cx-Select-Pull</td>
<td>I-CSCF</td>
<td>HSS</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>4. Cx-Query Resp/Cx-Select-Pull Resp</td>
<td>HSS</td>
<td>I-CSCF</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>5. Register</td>
<td>I-CSCF</td>
<td>S-CSCF</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>6. Cx-Pull/Cx-Pull</td>
<td>S-CSCF</td>
<td>HSS</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>7. Cx-Pull/Cx-Pull Response</td>
<td>HSS</td>
<td>S-CSCF</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>8. 200 OK</td>
<td>S-CSCF</td>
<td>I-CSCF</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>9. 200 OK</td>
<td>I-CSCF</td>
<td>UFA_GW</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>10. 200 OK</td>
<td>I-CSCF</td>
<td>UFA_GW</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Proxy Binding Update</td>
<td>UFA_GW</td>
<td>LMA</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Proxy Binding Acknowledgment</td>
<td>LMA</td>
<td>UFA_GW</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

The SIP and non-SIP (HTTP get) session establishment procedures are presented in the followings for HIP and PMIP based signalling schemes. For HIP, the HIP host associations and IPsec security associations must be established before application level session establishment occurs. Phipmncn gives the probability that the MN does not have an established HIP host association with the CN (or CN’s UFA_GW). Phipufacn gives the probability that MN’s UFA does not have an established HIP association with the CN (or CN’s UFA_GW). In case of having HIP and IPsec association between the MN’s UFA_GW and the CN or the CN’s UFA_GW (with probability 1-Phipufacn), then only a HIP update procedure is required instead of HIP BEX between the MN’s UFA_GW and the CN or the CN’s UFA_GW.

SIP INVITE procedure is needed for SIP applications. We took the example of a VoIP call. For non-SIP application, we supposed a simple HTTP request.
In the followings, the handover procedures for single-interface MNs, in case of option 3, are presented for HIP and PMIP based signalling schemes, respectively. Option 3 means that no cross optimization is made between SIP SDP update, and the 802.21 + HIP/PMIP handover. PMIP and HIP are responsible for L3 mobility handling. IEEE 802.21 is responsible for L2 handover preparation, and handover related signalling. The red messages indicate the messages causing service interruption. The SIP re-INVITE procedure is needed only for SIP sessions, when SDP must be updated. L2 attachment can include many messages responsible for L2 attachment, excluding L2 authentication. The L2 re-authentication with the new L2PoA is assumed to be done with ERP.

Pmiis gives the probability that the S_UFA_GW has not the information of its neighbours (candidate L2PoAs, T_UFA_GWs) in its local IS database, hence it needs to exchange information with the MIIS entity in the UFA core. N2N_HO_Query_Resources messages are sent to every neighbour UFA_GW.
(L2PoA) of the S_UFA_GW. Ncandidates gives the number of T_UFA_GWs (L2PoAs), from whom the L2 resource availability information must be collected before handover decision. IndTufa indicates whether T_UFA_GW has already an established HIP host association and IPsec SA pair with the MN and the MN's active peers or not. If it is 1, it means that the T_UFA_GW must establish HIP and IPsec associations with at least one of these entities. PT1mn gives the probability that the T_UFA_GW has not a HIP host association and IPsec SA pair with the MN, hence Type-1 HIP delegation service of the S_UFA_GW is needed to establish these associations between the T_UFA_GW and the MN. PT1r gives the same probability for the T_UFA_GW and MN’s RVS relationship. PT1cn gives the probability that T_UFA_GW has not already a HIP and IPsec association with the MN’s CN or the MN’s CN’s UFA_GW. Ncn gives the number of sessions of the MN with CNs that were decided to be handed off to the T_UFA_GW. In case of single-interface MN, Ncn is the number of active sessions of the MN with CNs. PT2r gives the probability that T_UFA_GW updates the location of the MN in MN'sRVS. In case of multi-interface MNs, it could be possible that only some sessions are handed off to T_UFA_GW, but the new CNs will still be directed to the S_UFA_GW of the MN, hence there is no need for location update in the RVS. For single-interface MNs, PT2r=1. PSDPupdate gives the probability that the SDP must be updated for a handed off SIP session. Ncn in that case gives the number of SIP sessions handed off.
<table>
<thead>
<tr>
<th>Message name</th>
<th>src</th>
<th>dst</th>
<th>number of messages per inter-UFA_GW handoff</th>
<th>network part</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIP Handover Initiation</td>
<td>S_UFA_GW</td>
<td>MN</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>HIP Handover Preparation</td>
<td>S_UFA_GW</td>
<td>MN</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>HIP Handover Decision</td>
<td>T_UFA_GW</td>
<td>S_UFA_GW</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>HIP Handover Execution</td>
<td>S_UFA_GW</td>
<td>MN</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>HIP Handover Completion</td>
<td>S_UFA_GW</td>
<td>MN</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

**Message Details**

- **Message name**: The name of the message.
- **src**: The source of the message.
- **dst**: The destination of the message.
- **Network part**: The part of the network where the message is sent.
- **number of messages per inter-UFA_GW handoff**: The number of messages sent per inter-UFA_GW handoff.

**Example Messages**

- **HIP Handover Initiation**: Initiates the handover process.
- **HIP Handover Preparation**: Prepares for the handover.
- **HIP Handover Decision**: Makes the decision to handover.
- **HIP Handover Execution**: Executes the handover.
- **HIP Handover Completion**: Completes the handover process.

© 2010 Eurescom participants in study P1857

EDIN 0586-1857
The following message traces show an optimized handover procedure, option 3. The SIP re-INVITE for SDP update is made before physical handover, hence the service interruption time for handed off SIP sessions requiring SDP update contains only L2 re-attachment and L2 fast re-authentication with ERP.
<table>
<thead>
<tr>
<th>Message name</th>
<th>src</th>
<th>dst</th>
<th>network part</th>
<th>number of messages per inter-UFA_GW handoff</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Handover Initiation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MIH_Link_Configure_Thresholds request</td>
<td>S_UFA_GW</td>
<td>MN</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>MIH_Link_Configure_Thresholds response</td>
<td>MN</td>
<td>S_UFA_GW</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>MIH_Link_Parameters_Report indication</td>
<td>MN</td>
<td>S_UFA_GW</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>MIH_Link_Going_Down indication</td>
<td>MN</td>
<td>S_UFA_GW</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td><strong>Handover Preparation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MIH_Det_Information request</td>
<td>S_UFA_GW</td>
<td>MIB</td>
<td></td>
<td>2 Pmils</td>
</tr>
<tr>
<td>MIH_Det_Information reply</td>
<td>MIB</td>
<td>S_UFA_GW</td>
<td></td>
<td>2 Pmils</td>
</tr>
<tr>
<td>MIH_Net_HO_Candidate_Query request</td>
<td>S_UFA_GW</td>
<td>MN</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>MIH_Net_HO_Candidate_Query response</td>
<td>MN</td>
<td>S_UFA_GW</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>MIH_N2N_HO_Query_Resources request</td>
<td>S_UFA_GW</td>
<td>T_UFA_GW</td>
<td></td>
<td>3 Ncandidates</td>
</tr>
<tr>
<td>MIH_N2N_HO_Query_Resources response</td>
<td>T_UFA_GW</td>
<td>S_UFA_GW</td>
<td></td>
<td>3 Ncandidates</td>
</tr>
<tr>
<td><strong>Handover Decision</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIP_UPDATE: Type 2 Mandated Action Request for handing off MN</td>
<td>S_UFA_GW</td>
<td>T_UFA_GW</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>HIP_UPDATE: Bulk Type 1 Delegation Action Request</td>
<td>T_UFA_GW</td>
<td>S_UFA_GW</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>HIP_UPDATE: Type 1 Mandated Request to Create HP and IPSec states for T_UFA_GW</td>
<td>S_UFA_GW</td>
<td>MN</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>HIP_UPDATE: Type 1 Mandated Response, HP and IPSec states created for T_UFA_GW</td>
<td>S_UFA_GW</td>
<td>MN</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>HIP_UPDATE: Type 1 Mandated Request to Create HP and IPSec states for T_UFA_GW</td>
<td>S_UFA_GW</td>
<td>MN</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>HIP_UPDATE: Type 1 Mandated Response, HP and IPSec states created for T_UFA_GW</td>
<td>S_UFA_GW</td>
<td>MN</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>HIP_UPDATE: Type 1 Mandated Request to Create HP and IPSec states for T_UFA_GW</td>
<td>S_UFA_GW</td>
<td>MN</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>HIP_UPDATE: Type 1 Mandated Response, HP and IPSec states created for T_UFA_GW</td>
<td>S_UFA_GW</td>
<td>MN</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>HIP_UPDATE: Type 1 Mandated Request to Create HP and IPSec states for T_UFA_GW</td>
<td>S_UFA_GW</td>
<td>MN</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>HIP_UPDATE: Type 1 Mandated Response, HP and IPSec states created for T_UFA_GW</td>
<td>S_UFA_GW</td>
<td>MN</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td><strong>Handover Execution</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP RE-INVITE</td>
<td>S_UFA_GW</td>
<td>MN</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>SIP UPDATE</td>
<td>S_UFA_GW</td>
<td>T_UFA_GW</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>SIP UPDATE</td>
<td>S_UFA_GW</td>
<td>S-CSCF</td>
<td></td>
<td>2 Ncn*PSDPupdate</td>
</tr>
<tr>
<td>SIP UPDATE</td>
<td>S-CSCF</td>
<td>CN_UFA_GW</td>
<td></td>
<td>6 Ncn*PSDPupdate</td>
</tr>
<tr>
<td>SIP UPDATE</td>
<td>CN_UFA_GW</td>
<td>CN</td>
<td></td>
<td>6 Ncn*PSDPupdate</td>
</tr>
<tr>
<td>SIP UPDATE</td>
<td>CN_UFA_GW</td>
<td>CN</td>
<td></td>
<td>6 Ncn*PSDPupdate</td>
</tr>
<tr>
<td>SIP UPDATE</td>
<td>S-CSCF</td>
<td>CN_UFA_GW</td>
<td></td>
<td>6 Ncn*PSDPupdate</td>
</tr>
<tr>
<td>SIP UPDATE</td>
<td>CN_UFA_GW</td>
<td>CN</td>
<td></td>
<td>6 Ncn*PSDPupdate</td>
</tr>
<tr>
<td>EAP-Initiate/Re-auth</td>
<td>MN</td>
<td>PoA</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>EAP-Initiate/Re-auth</td>
<td>PoA</td>
<td>local AAA</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>EAP-Finish/Re-auth</td>
<td>local AAA</td>
<td>PoA</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>EAP-Finish/Re-auth</td>
<td>PoA</td>
<td>MN</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td><strong>Handover Completion</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RE-INVITE</td>
<td>MN</td>
<td>T_UFA_GW</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>RE-INVITE</td>
<td>T_UFA_GW</td>
<td>MN</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>HIP_UPDATE: Type 2 Delegation Mandated Request to Update the Routing of MN's sessions</td>
<td>S_UFA_GW</td>
<td>T_UFA_GW</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>HIP_UPDATE: Type 2 Delegation Mandated Response to Update the Routing of MN's sessions</td>
<td>T_UFA_GW</td>
<td>S_UFA_GW</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>HIP_UPDATE</td>
<td>S_UFA_GW</td>
<td>T_UFA_GW</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>HIP_UPDATE</td>
<td>S_UFA_GW</td>
<td>T_UFA_GW</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td><strong>Handover Completion</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MN</td>
<td>T_UFA_GW</td>
<td>MN</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>MN</td>
<td>T_UFA_GW</td>
<td>MN</td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

**Context Transfer Data** (IPsec, HP states created for T_UFA_GW)

- Context Transfer Data Request | T_UFA_GW | S_UFA_GW |              | 3                                           |
- Context Transfer Data Response | T_UFA_GW | S_UFA_GW |              | 3                                           |
- HIP_UPDATE: Type 2 Delegation, Mandated Request to create HP states for MN | T_UFA_GW | RVS |              | 2 PTdosa                                    |
- HIP_UPDATE: Type 2 Delegation, Mandated Response HP states created for MN | RVS | T_UFA_GW |              | 2 PTdosa                                    |
- HIP_UPDATE: Type 2 Delegation, Mandated Request to create HP states for MN | T_UFA_GW | RVS |              | 2 PTdosa                                    |
- HIP_UPDATE: Type 2 Delegation, Mandated Response HP states created for MN | RVS | T_UFA_GW |              | 2 PTdosa                                    |
- HIP_UPDATE: Type 2 Delegation, Mandated Request to create HP states for MN | T_UFA_GW | CN's_UFA_GW |              | 4 Ncn                                       |
- HIP_UPDATE: Type 2 Delegation, Mandated Response HP states created for MN | CN's_UFA_GW | T_UFA_GW |              | 4 Ncn                                       |
- **Handover Execution** |               |              |              |                                             |
- SIP RE-INVITE | S_UFA_GW | MN |              | 1                                           |
- SIP UPDATE | S_UFA_GW | T_UFA_GW |              | 1                                           |
- SIP UPDATE | S_UFA_GW | S-CSCF |              | 2 Ncn*PSDPupdate                            |
- SIP UPDATE | S-CSCF | CN_UFA_GW |              | 6 Ncn*PSDPupdate                            |
- SIP UPDATE | CN_UFA_GW | CN |              | 6 Ncn*PSDPupdate                            |
- SIP UPDATE | CN_UFA_GW | CN |              | 6 Ncn*PSDPupdate                            |
- SIP UPDATE | S-CSCF | CN_UFA_GW |              | 6 Ncn*PSDPupdate                            |
- SIP UPDATE | CN_UFA_GW | CN |              | 6 Ncn*PSDPupdate                            |
- EAP-Initiate/Re-auth | MN | PoA |              | 1                                           |
- EAP-Initiate/Re-auth | PoA | local AAA |              | 1                                           |
- EAP-Finish/Re-auth | local AAA | PoA |              | 1                                           |
- EAP-Finish/Re-auth | PoA | MN |              | 1                                           |
- **Handover Completion** |               |              |              |                                             |
- RE-INVITE | MN | T_UFA_GW |              | 1                                           |
- RE-INVITE | T_UFA_GW | MN |              | 1                                           |
- HIP_UPDATE: Type 2 Delegation Mandated Request to Update the Routing of MN's sessions | S_UFA_GW | T_UFA_GW |              | 1                                           |
- HIP_UPDATE: Type 2 Delegation Mandated Response to Update the Routing of MN's sessions | T_UFA_GW | S_UFA_GW |              | 1                                           |
- HIP_UPDATE | S_UFA_GW | T_UFA_GW |              | 1                                           |
- HIP_UPDATE | S_UFA_GW | T_UFA_GW |              | 1                                           |
- **Handover Completion** |               |              |              |                                             |
- MN | T_UFA_GW | MN |              | 1                                           |
- MN | T_UFA_GW | MN |              | 1                                           |
### Handover Initiation

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Source</th>
<th>Destination</th>
<th>P1857</th>
<th>Pmiis</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIH_Link_Configure_Thresholds request</td>
<td>S_UFA_GW</td>
<td>MN</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MIH_Link_Configure_Thresholds response</td>
<td>MN</td>
<td>S_UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MIH_Link_Parameters_Report indication</td>
<td>MN</td>
<td>S_UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MIH_Link_Going_Down indication</td>
<td>MN</td>
<td>S_UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

### Handover Preparation

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Source</th>
<th>Destination</th>
<th>P1857</th>
<th>Pmiis</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIH_Get_Information request</td>
<td>S_UFA_GW</td>
<td>MIS</td>
<td>2</td>
<td>Pmiis</td>
</tr>
<tr>
<td>MIH_Get_Information reply</td>
<td>MIS</td>
<td>S_UFA_GW</td>
<td>2</td>
<td>Pmiis</td>
</tr>
<tr>
<td>MIH_Handover_Ho_Candidate_Query request</td>
<td>S_UFA_GW</td>
<td>MN</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MIH_Handover_Ho_Candidate_Query response</td>
<td>MN</td>
<td>S_UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MIH_Handover_Ho_Query_Resources request</td>
<td>S_UFA_GW</td>
<td>T_UFA_GW</td>
<td>3</td>
<td>Pmiis</td>
</tr>
<tr>
<td>MIH_Handover_Ho_Query_Resources response</td>
<td>T_UFA_GW</td>
<td>S_UFA_GW</td>
<td>3</td>
<td>Pmiis</td>
</tr>
</tbody>
</table>

### Handover Decision

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Source</th>
<th>Destination</th>
<th>P1857</th>
<th>Pmiis</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIH_Handover_Commit request</td>
<td>MN</td>
<td>S_UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MIH_Handover_Commit request</td>
<td>S_UFA_GW</td>
<td>T_UFA_GW</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>MIH_Handover_Commit response</td>
<td>MN</td>
<td>S_UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Query about MN's profile</td>
<td>S_UFA_GW</td>
<td>LMA</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Proxy_Binding_Update Request</td>
<td>S_UFA_GW</td>
<td>LMA</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

### Proxy Binding Acknowledgment Message

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Source</th>
<th>Destination</th>
<th>P1857</th>
<th>Pmiis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy_Binding_Update Request</td>
<td>S_UFA_GW</td>
<td>S_UFA_GW</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

### Handover Execution

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Source</th>
<th>Destination</th>
<th>P1857</th>
<th>Pmiis</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP_INVITE</td>
<td>S_UFA_GW</td>
<td>MN</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>ACK</td>
<td>S_UFA_GW</td>
<td>MN</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>SIP_INVITE</td>
<td>S_UFA_GW</td>
<td>S-CSCF</td>
<td>2</td>
<td>Non/PSDPupdate</td>
</tr>
<tr>
<td>SIP_INVITE</td>
<td>S-CSCF</td>
<td>CN_UFA_GW</td>
<td>6</td>
<td>Non/PSDPupdate</td>
</tr>
<tr>
<td>SIP_INVITE</td>
<td>CN_UFA_GW</td>
<td>CN</td>
<td>7</td>
<td>Non/PSDPupdate</td>
</tr>
<tr>
<td>SIP_INVITE</td>
<td>CN</td>
<td>CN_UFA_GW</td>
<td>7</td>
<td>Non/PSDPupdate</td>
</tr>
<tr>
<td>SIP_INVITE</td>
<td>CN_UFA_GW</td>
<td>S-CSCF</td>
<td>6</td>
<td>Non/PSDPupdate</td>
</tr>
<tr>
<td>SIP_INVITE</td>
<td>S-CSCF</td>
<td>CN_UFA_GW</td>
<td>2</td>
<td>Non/PSDPupdate</td>
</tr>
<tr>
<td>ACK</td>
<td>S-UFA_GW</td>
<td>S-CSCF</td>
<td>2</td>
<td>Non/PSDPupdate</td>
</tr>
<tr>
<td>ACK</td>
<td>S-CSCF</td>
<td>CN_UFA_GW</td>
<td>6</td>
<td>Non/PSDPupdate</td>
</tr>
<tr>
<td>ACK</td>
<td>CN_UFA_GW</td>
<td>CN</td>
<td>7</td>
<td>Non/PSDPupdate</td>
</tr>
</tbody>
</table>

### L2 Attachment

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Source</th>
<th>Destination</th>
<th>P1857</th>
<th>Pmiis</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2 attachment</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

### EAP-Initiate/Re-auth Request

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Source</th>
<th>Destination</th>
<th>P1857</th>
<th>Pmiis</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP-Initiate/Re-auth Request</td>
<td>MN</td>
<td>PoA</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>EAP-Initiate/Re-auth Request</td>
<td>PoA</td>
<td>local AAA</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>EAP-Finish/Re-auth Request</td>
<td>local AAA</td>
<td>PoA</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>EAP-Finish/Re-auth Request</td>
<td>PoA</td>
<td>MN</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

### Proxy Binding Update

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Source</th>
<th>Destination</th>
<th>P1857</th>
<th>Pmiis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy_Binding_Update Request</td>
<td>T_UFA_GW</td>
<td>LMA</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

### Proxy Binding Acknowledgment

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Source</th>
<th>Destination</th>
<th>P1857</th>
<th>Pmiis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy_Binding_Update Request</td>
<td>T_UFA_GW</td>
<td>LMA</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

### Handover Completion

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Source</th>
<th>Destination</th>
<th>P1857</th>
<th>Pmiis</th>
</tr>
</thead>
<tbody>
<tr>
<td>RE_INVITE</td>
<td>MN</td>
<td>T_UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>200_OK</td>
<td>T_UFA_GW</td>
<td>MN</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>ACK</td>
<td>MN</td>
<td>T_UFA_GW</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MIH_Handover_Complete request</td>
<td>T_UFA_GW</td>
<td>S_UFA_GW</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>MIH_Handover_Complete response</td>
<td>S_UFA_GW</td>
<td>T_UFA_GW</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>
Annex H References


