3P-AAA Framework for UCWW

Dmitry Tairov, BEng.

Thesis submitted for the degree of Master of Engineering

Supervisors
Dr. Ivan Ganchev
Dr. Máirtín Ó Dróma,

Department of Electronic and Computer Engineering
University of Limerick, Ireland

Submitted to the University of Limerick, June, 2011
ABSTRACT

Third-Party Authentication, Authorization and Accounting Framework for Ubiquitous Consumer Wireless World

Dmitry Tairov

This thesis proposes a new approach to the management of the Authentication, Authorization and Accounting (AAA) function that forms a core part of many service provider networks. The principle idea outlined is to move this function under the supervision of the trusted Third Parties and independent of the Access Network Providers. This change would provide for additional flexibility through enabling users to switch their network providers depending on their current needs and the required quality of service levels. The key issue addressed in this thesis is the development of the signaling framework for the Third-Party AAA, which is an integral entity of the Ubiquitous Consumer Wireless World (UCWW) [1, 2] project.

A review of the currently existing Business Models and Technologies is performed in the introducing chapters of the thesis. The key issue here is to investigate what currently existing technologies and protocols could be used to provide the base for the development of the 3P-AAA. Some of the signaling protocols along with security features are already implemented by a number of the network providers and can be inherited by the 3P-AAA. These features include signaling protocols like Diameter and PANA, as well as security features provided by the Extensible Authentication Protocol (EAP) and the X.509 Certificates.

Based on the researched material the 3P-AAA framework is described along with its corresponding entities and interfaces. Based on the discussion of the possible use scenarios and the requirements drawn from them, the 3P-AAA signaling protocol messages and novel Attribute-Value Pairs (AVPs) are outlined. The concluding chapter of the thesis aims to outline the implementation related issues that include the possible software protocol stacks and the simulation tools.

The ideas related to the 3P-AAA design outlined in this thesis have also been disseminated through presentations at international research conference meetings, namely Globe Forum Dublin and European Cooperation in Science and Technology Wireless Networking for Moving Object (WiNeMO) meeting. Various other aspects have been described in the IEEE conference paper publications within the upcoming 7th International Conference on Wireless Communications, Networking and Mobile Computing and the 5th International Conference on Next Generation Mobile Applications, Services and Technologies.
DECLARATION

I hereby declare that I am the sole author of this Master Thesis. I authorize University of Limerick to lend this Thesis to other institutions or individuals for the purpose of academic research.

I further authorize University of Limerick to reproduce this Master Thesis by photocopying or other means, in total or part, at the request of other institutions or individuals for the purpose of academic research.

Dmitry Tairov
ACKNOWLEDGEMENTS

I would like to thank my research supervisors, Dr Ivan Ganchev and Dr Máirtín ÓDroma, for their help and guidance. I am very thankful for the opportunity given to undertake the postgraduate studies especially in the difficult economic times present today.
On top of that I would like to express special gratitude to the Irish Research Council for Science, Engineering and Technology (IRCSET) for their financial support.
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Generic AAA Architecture</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>EAP Packet Format</td>
<td>9</td>
</tr>
<tr>
<td>3</td>
<td>EAP Pass Through</td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td>EAP over LAN</td>
<td>11</td>
</tr>
<tr>
<td>5</td>
<td>User Certificate signing</td>
<td>12</td>
</tr>
<tr>
<td>6</td>
<td>3-Way Authentication Procedure</td>
<td>13</td>
</tr>
<tr>
<td>7</td>
<td>PANA functional components</td>
<td>14</td>
</tr>
<tr>
<td>8</td>
<td>IMS Architecture</td>
<td>17</td>
</tr>
<tr>
<td>9</td>
<td>SIP Call Session</td>
<td>19</td>
</tr>
<tr>
<td>10</td>
<td>RADIUS Message Format</td>
<td>23</td>
</tr>
<tr>
<td>11</td>
<td>Diameter Relay Agent</td>
<td>25</td>
</tr>
<tr>
<td>12</td>
<td>Diameter Redirect Agent</td>
<td>26</td>
</tr>
<tr>
<td>13</td>
<td>Diameter Translation Agent</td>
<td>27</td>
</tr>
<tr>
<td>14</td>
<td>Diameter Header</td>
<td>27</td>
</tr>
<tr>
<td>15</td>
<td>AVP Header</td>
<td>28</td>
</tr>
<tr>
<td>16</td>
<td>3P-AAA framework</td>
<td>35</td>
</tr>
<tr>
<td>17</td>
<td>Session outline</td>
<td>39</td>
</tr>
<tr>
<td>18</td>
<td>Authentication and Authorization (Online Charging)</td>
<td>40</td>
</tr>
<tr>
<td>19</td>
<td>Authentication and Authorization (Offline Charging)</td>
<td>42</td>
</tr>
<tr>
<td>20</td>
<td>Service Delivery (Online Charging)</td>
<td>44</td>
</tr>
<tr>
<td>21</td>
<td>Service Delivery (Offline Charging)</td>
<td>46</td>
</tr>
<tr>
<td>22</td>
<td>Session Termination (Online Charging)</td>
<td>48</td>
</tr>
<tr>
<td>23</td>
<td>Session Termination (Offline Charging)</td>
<td>49</td>
</tr>
<tr>
<td>24</td>
<td>Abrupt Session Termination</td>
<td>50</td>
</tr>
<tr>
<td>25</td>
<td>ANP Re-Authentication and Re-Authorization (Online Charging)</td>
<td>51</td>
</tr>
<tr>
<td>26</td>
<td>ANP Re-Authorization Failure (Online Charging)</td>
<td>52</td>
</tr>
<tr>
<td>27</td>
<td>Successful Credit Replenishment</td>
<td>54</td>
</tr>
<tr>
<td>28</td>
<td>Unsuccessful Account Replenishment</td>
<td>55</td>
</tr>
<tr>
<td>29</td>
<td>Failover (ANP terminates session)</td>
<td>58</td>
</tr>
<tr>
<td>30</td>
<td>Failover (ANP continues granting services)</td>
<td>59</td>
</tr>
<tr>
<td>31</td>
<td>User Triggered HAC (Online Charging)</td>
<td>63</td>
</tr>
<tr>
<td>32</td>
<td>TSP/VASP Triggered HAC (Online Charging)</td>
<td>65</td>
</tr>
<tr>
<td>33</td>
<td>User triggered HAC with TSP change</td>
<td>66</td>
</tr>
<tr>
<td>34</td>
<td>TSP HAC signalling (Online Charging)</td>
<td>67</td>
</tr>
<tr>
<td>35</td>
<td>Access to teleservice(s) through different ANPs</td>
<td>68</td>
</tr>
<tr>
<td>36</td>
<td>Multiple ANP session</td>
<td>69</td>
</tr>
<tr>
<td>37</td>
<td>Value Added Services framework</td>
<td>71</td>
</tr>
<tr>
<td>38</td>
<td>Service Delivery Chaining Example</td>
<td>72</td>
</tr>
<tr>
<td>39</td>
<td>Service Delivery Chaining</td>
<td>73</td>
</tr>
<tr>
<td>40</td>
<td>Chained Service Session Termination</td>
<td>74</td>
</tr>
<tr>
<td>41</td>
<td>3P-AAA and IMS integration</td>
<td>75</td>
</tr>
<tr>
<td>42</td>
<td>3P-AAA signalling protocol stack</td>
<td>79</td>
</tr>
</tbody>
</table>
LIST OF TABLES

Table I: Base Diameter message codes ................................................................. 28
Table II: VAS classification (Balasubramanian et al.) ............................................. 70
Table III: Comparing signalling protocols ............................................................. 77
Table IV: 3P-AAA signalling messages ................................................................ 79
# LIST OF ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2G</td>
<td>Second Generation</td>
</tr>
<tr>
<td>3G</td>
<td>Third Generation</td>
</tr>
<tr>
<td>3GPP</td>
<td>3rd Generation Partnership Project</td>
</tr>
<tr>
<td>AAA</td>
<td>Authentication, Authorization and Accounting</td>
</tr>
<tr>
<td>ABC&amp;S</td>
<td>Always Best Connected and Served</td>
</tr>
<tr>
<td>ACE</td>
<td>Adaptive Communication Environment</td>
</tr>
<tr>
<td>ADA</td>
<td>Advertisement, Discovery and Association</td>
</tr>
<tr>
<td>AKA</td>
<td>Authentication and Key Agreement</td>
</tr>
<tr>
<td>ANI</td>
<td>Application-to-Network Interface</td>
</tr>
<tr>
<td>ANP</td>
<td>Access Network Provider</td>
</tr>
<tr>
<td>ASM</td>
<td>Application Specific Module</td>
</tr>
<tr>
<td>AVP</td>
<td>Attribute Value Pair</td>
</tr>
<tr>
<td>AuC</td>
<td>Authentication Centre</td>
</tr>
<tr>
<td>C&amp;B</td>
<td>Charging and Billing</td>
</tr>
<tr>
<td>CAMEL</td>
<td>Customized Applications for Mobile Network Enhanced Logic</td>
</tr>
<tr>
<td>CBM</td>
<td>Consumer-centric Business Model</td>
</tr>
<tr>
<td>CDMA</td>
<td>Code Division Multiple Access</td>
</tr>
<tr>
<td>CDR</td>
<td>Charging Detail Records</td>
</tr>
<tr>
<td>CHAP</td>
<td>Challenge-Handshake Authentication Protocol</td>
</tr>
<tr>
<td>CSCF</td>
<td>Call/Session Control Function</td>
</tr>
<tr>
<td>DECT</td>
<td>Digital Enhanced Cordless Telecommunication</td>
</tr>
<tr>
<td>E2E HAC</td>
<td>End to End Hot Access Change</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>EAPOL</td>
<td>EAP over LAN</td>
</tr>
<tr>
<td>EDGE</td>
<td>Enhanced Data rates for GSM Evolution</td>
</tr>
<tr>
<td>EIR</td>
<td>Equipment Information Register</td>
</tr>
<tr>
<td>EP</td>
<td>Enforcement Point</td>
</tr>
<tr>
<td>FA</td>
<td>Foreign Agent</td>
</tr>
<tr>
<td>FSM</td>
<td>Finite State Machine</td>
</tr>
<tr>
<td>GNU</td>
<td>GNU’s not Unix</td>
</tr>
<tr>
<td>GPRS</td>
<td>General Packet Radio Service</td>
</tr>
<tr>
<td>GSM</td>
<td>General System for Mobile communication</td>
</tr>
<tr>
<td>HA</td>
<td>Home Agent</td>
</tr>
<tr>
<td>HAC</td>
<td>Hot Access network Change</td>
</tr>
<tr>
<td>HLR</td>
<td>Home Location Register</td>
</tr>
<tr>
<td>HMIP</td>
<td>Hierarchical Mobile IP</td>
</tr>
<tr>
<td>HSS</td>
<td>Home Subscribe Service</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>IANA</td>
<td>Internet Assigned Number Authority</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronic Engineers</td>
</tr>
<tr>
<td>IETF</td>
<td>International Engineering Task Force</td>
</tr>
<tr>
<td>IMS</td>
<td>IP Multimedia Subsystem</td>
</tr>
<tr>
<td>IM-SSF</td>
<td>IP Multimedia Service Switch Function</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LRF</td>
<td>Location Retrieval Function</td>
</tr>
<tr>
<td>MAHO</td>
<td>Mobile Assisted HandOver</td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest algorithm 5</td>
</tr>
<tr>
<td>MIP</td>
<td>Mobile IP</td>
</tr>
<tr>
<td>MMD</td>
<td>MultiMedia Domain</td>
</tr>
<tr>
<td>MVNO</td>
<td>Mobile Virtual Network Operator</td>
</tr>
<tr>
<td>NASREQ</td>
<td>Network Access Server Requirements</td>
</tr>
<tr>
<td>NGN</td>
<td>Next Generation Networks</td>
</tr>
<tr>
<td>NNI</td>
<td>Network-to-Network Interface</td>
</tr>
<tr>
<td>OCF</td>
<td>Online Charging Function</td>
</tr>
<tr>
<td>OSA</td>
<td>Open Service Access</td>
</tr>
<tr>
<td>OTT</td>
<td>Over The Top</td>
</tr>
<tr>
<td>PAA</td>
<td>PANA Authentication Agent</td>
</tr>
<tr>
<td>PaC</td>
<td>PANA Client</td>
</tr>
<tr>
<td>PAN</td>
<td>Personal Area Networks</td>
</tr>
<tr>
<td>PANA</td>
<td>Protocol for carrying Authentication for Network Access</td>
</tr>
<tr>
<td>PAP</td>
<td>PPP Authentication Protocol</td>
</tr>
<tr>
<td>PDA</td>
<td>Personal Digital Assistant</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>POSIX</td>
<td>Portable Operation System for Unix</td>
</tr>
<tr>
<td>PPP</td>
<td>Point-to-Point Protocol</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial In User Service</td>
</tr>
<tr>
<td>RFC</td>
<td>Request for Commence</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Shamir &amp; Adelman</td>
</tr>
<tr>
<td>SAX</td>
<td>Simple API for XML</td>
</tr>
<tr>
<td>SCTP</td>
<td>Stream Control Transmission Protocol</td>
</tr>
<tr>
<td>SE</td>
<td>Service Equipment</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Terminal Access Controller Access-Control System Plus</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TRC</td>
<td>Telecommunication Research Centre</td>
</tr>
<tr>
<td>TSP</td>
<td>Teleservice Provider</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>UCWW</td>
<td>Ubiquitous Consumer Wireless World</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunication System</td>
</tr>
<tr>
<td>VASP</td>
<td>Value Added Service Provider</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Networks</td>
</tr>
<tr>
<td>WAP</td>
<td>Wireless Application Protocol</td>
</tr>
<tr>
<td>WBC</td>
<td>Wireless Broadcast Channels</td>
</tr>
<tr>
<td>WiMAX</td>
<td>Wireless Interoperability for Mobile Access</td>
</tr>
<tr>
<td>WiNeMO</td>
<td>Wireless Networking for Moving Objects</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
</tbody>
</table>
CONTENTS

Abstract ................................................................................................................................. i

Third-Party Authentication, Authorization and Accounting Framework for
Ubiquitous Consumer Wireless World .................................................................................. i

Declaration ............................................................................................................................. ii

Acknowledgements .............................................................................................................. iii

List of Figures ....................................................................................................................... iv

List of Tables ........................................................................................................................ v

List of Abbreviations .......................................................................................................... vi

Chapter 1 ............................................................................................................................. 1

Introduction ........................................................................................................................... 1

1.1 Introduction ..................................................................................................................... 1

1.2 Business Models ........................................................................................................... 2

1.2.1 Mobile Virtual Network Operator (MVNO) Business Model.............................. 2

1.2.2 Two-Sided Telecoms Business Model ................................................................... 2

1.2.3 Over the Top (OTT) Business Model ................................................................... 3

1.2.4 The “Freemium” Business Model ......................................................................... 3

1.2.5 The “Smart Pipe” Business Model ....................................................................... 3

1.3 Research Objectives ..................................................................................................... 3

1.4 Thesis Organization ...................................................................................................... 4

1.5 Conclusion ..................................................................................................................... 5

Chapter 2 ............................................................................................................................. 6

AAA and Security Frameworks ............................................................................................ 6

2.1 Introduction ..................................................................................................................... 6

2.2 Security Services .......................................................................................................... 6

2.3 Generic AAA Architecture .......................................................................................... 7

2.4 Extensible Authentication Protocol (EAP) Framework ............................................... 9

2.5 Public Key Infrastructure X. 509 Certificates Framework ......................................... 11

2.5.1 Authentication Procedure ....................................................................................... 12

2.5.2 Implementation Issues ............................................................................................ 13

2.6 Protocol for carrying Authentication for Network Access (PANA) Architecture ......... 14
2.7 IP Multimedia Subsystem (IMS) Infrastructure ........................................... 15
  2.7.1 IMS Architectural Overview ................................................................ 16
2.8 Session Initiation Protocol Framework ....................................................... 18
2.9 Conclusion .............................................................................................. 20

Chapter 3 ...................................................................................................... 21
AAA Protocols- RADIUS and Diameter ......................................................... 21
  3.1 Introduction .......................................................................................... 21
  3.2 Remote Authentication Dial-In User Service (RADIUS) ......................... 21
    3.2.1 RADIUS Message Format .............................................................. 22
    3.2.2 RADIUS Accounting ................................................................. 23
  3.3 Diameter ............................................................................................... 24
    3.3.1 Diameter nodes and agents ........................................................... 25
    3.3.2 Diameter Messages ..................................................................... 27
    3.3.3 Diameter Peers .......................................................................... 29
    3.3.4 Error Handling ........................................................................... 29
    3.3.5 Diameter Sessions ...................................................................... 30
    3.3.6 Accounting .................................................................................. 31
    3.3.7 Diameter Credit Control ............................................................. 31
    3.3.8 Diameter’s Evolution ................................................................... 32
  3.4 Conclusion ............................................................................................. 33

Chapter 4 ...................................................................................................... 34
3P-AAA Framework ....................................................................................... 34
  4.1 Introduction .......................................................................................... 34
  4.2 Entities ................................................................................................ 35
  4.3 3P-AAA Interfaces ............................................................................. 36
    4.3.1 Interface ‘a’ ................................................................................ 36
    4.3.2 Interface ‘b’ .............................................................................. 37
    4.3.3 Interface ‘c’ .............................................................................. 37
  4.4 3P-AAA Scenarios ............................................................................ 38
    4.4.1 Basic Signalling Scenarios .......................................................... 38
    4.4.2 HAC Related Scenarios .............................................................. 60
    4.4.3 Novel 3P-AAA Scenarios ............................................................ 65
  4.5 3P-AAA and IMS integration ............................................................. 74
4.6 Conclusion ........................................................................................................... 75
Chapter 5 ................................................................................................................ 77
3P-AAA Signalling ................................................................................................... 77
  5.1 Introduction ....................................................................................................... 77
  5.2 3P-AAA Protocol Stack ................................................................................... 77
  5.3 Messages and AVPs ....................................................................................... 79
    5.3.1 Messages over Interface ‘a’ ...................................................................... 80
    5.3.2 Messages over Interface ‘b’ ...................................................................... 85
    5.3.3 Messages over Interface ‘c’ ...................................................................... 87
  5.4 3P-AAAA AVPs ............................................................................................. 94
  5.5 Conclusion ..................................................................................................... 97
Chapter 6 ................................................................................................................ 98
Implementation Issues .......................................................................................... 98
  6.1 Protocol Stacks .............................................................................................. 98
    6.1.1 OpenDiameter ......................................................................................... 99
    6.1.2 OpenBlox ............................................................................................... 100
    6.1.3 JDiameter ............................................................................................... 100
    6.1.4 Cpana .................................................................................................... 101
  6.2 Simulation Issues .......................................................................................... 101
  6.3 Conclusion .................................................................................................... 102
Chapter 7 ................................................................................................................ 103
Conclusions and Future Work ............................................................................ 103
  Research outcomes published to date .............................................................. 106
References ............................................................................................................. 108
CHAPTER 1

INTRODUCTION

1.1 Introduction

Ubiquitous Consumer Wireless World (UCWW) is aimed at the creation of the novel wireless environment. What makes UCWW different from the currently existing frameworks is a different business model approach. UCWW proposes to move away from the currently deployed Subscriber-based Business Model (SBM), where every user needs to subscribe to a service in order to use it, to the Consumer-centric Business Model [1]. The way to achieve this is seen through the move of the Authentication, Authorization and Accounting (AAA) function under the supervision of the trusted Third Party Providers. This strategic innovation would enable consumers to gain access to the network and teleservices without the need for the long-term subscription with the corresponding service providing bodies

Wireless telecommunication industry has seen many stages of development in the last few decades. These can be traced from the deployment of the analog networks all the way to the creation of the wireless 3G networks that are currently introduced to the wide public around the world, and with plans for evolving into 4G wireless communications at an advanced stage. Traditionally wireless networks were concerned with two types of services: voice and data. What we currently experience is a major shift towards all-IP networks and demand for higher speed and quality of service (QoS). However, it should be noted that the advances in the telecommunication industry have mostly been technology driven. UCWW and the deployment of the CBM aim to create a more liberal and open environment that in turn would be stimulation to the emergence of the new business opportunities.

The rest of this chapter looks at some of the currently existing business models and trends. It also focuses on the general research objectives of the thesis which aim at the discussion of the principle milestones in the development of the 3P-AAA framework. The last section of this introductory chapter describes the outline of the thesis.
1.2 Business Models

This section looks briefly at the business models currently employed in the industry [3]. The traditional business model heavily relies on voice revenues. However, currently there is a lot of demand for data services and more personified packaged service bundles. Operators are faced with stiff competition from Over the Top (OTT) applications and content providers such as Facebook, Twitter etc. New business models should enable the move of the decision-making power towards customers and application providers and away from the traditional service providers.

1.2.1 Mobile Virtual Network Operator (MVNO) Business Model

In this business model wireless network service providers lease their networks to other carriers. Thus Mobile Virtual Network Operators (MVNO) cannot participate in the provision of the spectrum to customers but they can generate revenues through innovating, operating and selling mobile services. While traditionally for wireless network provider provision of spectrum is seen as a primary task and provision of additional services is only an auxiliary source of revenue, for MVNO service provision becomes a specialization and they are able to target certain niche markets. The resurgence of MVNOs is based on the new business model emphasizing delivery of total solutions with wireless as part of the package. An example is the free Amazon Whispernet content service bundled with a Kindle reading device [4].

1.2.2 Two-Sided Telecoms Business Model

With development of the wireless broadband networks, operators will have the option of not only bundling voice, broadband data and media content, but also to leverage their assets to link upstream customers to downstream customers. Upstream companies may include industries and communities providing services to downstream customers i.e. traditional wireless consumers where operator plays role of the middle man. To move into two-sided telecom business model, wireless operators need to:

- Be more consumer orientated
- Modernize their platforms to support different charging models and to control exposure to their assets
- Learn from success of companies such as Facebook, Google and Apple which were successful at providing their application store solutions and support
1.2.3 Over the Top (OTT) Business Model

Over the last few years there has been an increase in the competition between “over-the-top” service providers versus the carriers. The term “over-the-top” refers to the provision of services on top of the internet connection independent of the subscriber’s ISP. The problem with this thriving business model is that OTT providers are dispersed and their service platforms are not standardized.

1.2.4 The “Freemium” Business Model

This model focuses on the provision of a free basic service where charging is only applied to the premium content. Basic services might not necessarily be web applications but also content such as software, games etc. This model is very well suited for innovative services that the people are not familiar with. There is a greater incentive to try out new things if they are free of charge.

1.2.5 The “Smart Pipe” Business Model

This term refers to an operator’s network which leverages existing or unique service capabilities as well as the operator’s own customer relationships to provide value beyond data connectivity [5]. In other word it is an ability of an operator to offer added value to unique types of services.

As can be seen from the examples of the business models mentioned above, the Subscriber-based Business Model (SMB) dominates the telecommunication market.

1.3 Research Objectives

A key role in the AAA management is proposed to be given to a 3P-AAA not integral to the traditional wireless communications. This alternative is attractive in that it separates out this administration and management of consumers’ one-stop-shop accounting system and the various business agreements with other parties from the business of supplying a wireless access network service [1, 2]. All types of teleservice providers (TSPs) and access network providers (ANPs) will be able to offer their services to mobile users through the business agreements each and all will have with third-party AAA service providers (3P-AAA-SPs), who become the central players in UCWW. Mobile users will have arrangements with one or more 3P-AAA-SP, just as they have one or more credit cards, and similarly through this entity will receive periodic itemized bills for all services used. The mobile users’ choice of 3P-AAA-SPs at any time for any service will be dictated by decision processes similar to those in deciding which credit card to use for a particular bill.
CBM’s 3P-AAA infrastructure follows guidelines for the NGN systems[3], as it centralizes customer and product data within 3P-AAA framework. 3P-AAA would create a better environment for the enforcement of converged charging since all the charging and billing takes place within 3P-AAA and not within numerous access and teleservice providers. Overall, it would create a stimulating environment for consumer centric service personalization.

The following can be considered the main objectives of the research described in this thesis:

- Creation of a foundational infrastructure that would enable the core AAA functionality to be placed in the hands of ‘non-communications third-party management companies’. Success here will lead to a radical re-structuring of how wireless communication services may be created, deployed, delivered and paid for and to a real possibility to satisfy the legitimate modern consumer expectation of being able to move back and forth readily among access networks/providers at any time for any and all services. Furthermore, such an attribute is a major contribution towards the realisation of the ‘always best connected and best served’ (ABC&S) capability for the consumers [1, 2].

- Investigation of how the newly created infrastructure can be integrated with technologies and frameworks widely deployed throughout the industry today. These include evaluation of the interfaces and signalling infrastructure employed by 3GPP IP Multimedia Subsystems (IMS). IMS presents an interesting case study since it allows for the deployment of third-party Value Added Services.

- Development of a 3P-AAA interface architecture - three main application-layer interfaces are foreseen: Mobile User↔ANP/TSP (a); Mobile User↔3P-AAA-SP (b); and ANP/TSP↔3P-AAA-SP (c).

- Development of a 3P-AAA signalling protocol based on the evaluation of the possible interaction scenarios and signalling requirements - the IETF Diameter protocol is considered as a main candidate to carry the 3P-AAA signalling. However, adjustments of it for 3P-AAA will be required. The application autonomy would also help the process of developing the standards for the three indicated interfaces. In support of this the application capability range would include all necessary functionality with defined messages for 3P-AAA, purchaser transactions, mobility, user privacy, etc. [1, 2]

1.4 Thesis Organization

The rest of this thesis is organized as follows:
• Chapter 2 looks at the concepts and protocols related to the AAA. It also briefly looks at the architecture of the IP Multimedia Subsystems (IMS) that can serve as an example study case of the AAA framework.
• Chapter 3 focuses primarily on the two examples of the AAA signalling protocols- RADIUS and Diameter.
• Based on the ideas expressed in the previous chapters, chapter 4 draws an outline of the 3P-AAA framework. Principle interfaces and signalling scenarios describe the types of interactions that could be handled by this framework.
• Chapter 5 concentrates on the definition of the signalling messages and corresponding Attribute-Value Pairs (AVPs) based on the requirements outlined in chapter 4.
• Chapter 6 discuses implementation issues that need to be overcome in order to successfully implement outlined framework.
• Chapter 7 concludes this thesis.

1.5 Conclusion

This introductory chapter aims to introduce the key motives for the emergence of the proposed framework. Some of the key concepts related to UCWW, such as the difference between the SBM and the CBM are outlined. In order to demonstrate the contrast between the two business models, some of the currently existing and deployed business model variations of the SBM are given. A conclusion could be drawn from the description of the above-mentioned business models, that in general, there exists a need for new business opportunities among different service providers in order to continue generating revenues. Thus the emergence of the 3P-AAA framework could be beneficial not only to the consumer, but also to the service providers as it will create a stimulating environment for the emergence of these opportunities. At last, the principle objectives of the thesis are outlined that will be covered in more detail in the proceeding chapters.
CHAPTER 2

AAA AND SECURITY FRAMEWORKS

2.1 Introduction

Authentication, Authorization and Accounting is commonly used in telecommunication infrastructure to identify users, control access to data and keep track of the resources used. Thus the aim of this chapter is to provide an overview of the technical aspects involved in the provision of an adequate AAA service. Since 3P-AAA would require to carry sensitive data, security is one of the central issues. This chapter looks at the definition of the security services along with two security frameworks that will be considered for the 3P-AAA: the Extensible Authentication Protocol (EAP) and the X.509 Certificates. Additionally, the interfaces employed by the 3P-AAA would have to carry their data by means of some signalling protocol. Two signalling protocols, Session Initiation Protocol (SIP) and PANA, will be studied in order to see if these protocols or some of their features may be adapted by the 3P-AAA framework. In order to see how some of these technologies and protocols are being employed in the industry, the Third Generation Partnership IP Multimedia Subsystems (IMS) framework will be discussed as a study case example.

2.2 Security Services

A good AAA systems should be concerned with provision of reliable security services that would benefit not only the service provider but also an end-user. A number of security services can be identified [6]:

- Authentication-The authentication service is concerned with assuring that a communicating party is authentic, i.e., that it is what it claims to be. Authentication is accomplished via the claimant's presentation of an identifier and its corresponding credentials to the verifier. Examples of types of credentials are passwords, one-time tokens, digital certificates, and phone numbers (calling/called).
- Authorization (Access Control) - In the context of network security, access control is the ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.
Accounting- Accounting refers to the tracking of the consumption of network resources by users. This information may be used for management, planning, billing, or other purposes. Real-time accounting refers to accounting information that is delivered concurrently with the consumption of the resources. Batch accounting refers to accounting information that is saved until it is delivered at a later time. Typical information that is gathered in accounting is the identity of the user, the nature of the service delivered, when the service began, and when it ended.

Data Integrity- Integrity can apply to a stream of messages, a single message, or selected fields within a message. A connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent, with no duplication, insertion, modification, reordering, or replays. The destruction of data is also covered under this service. On the other hand, a connectionless integrity service, one that deals with individual messages without regard to any larger context, generally provides protection against message modification only.

Data Confidentiality- Confidentiality is the protection of transmitted data from passive attacks. With respect to the content of a data transmission, several levels of protection can be identified. The broadest service protects all user data transmitted between two users over a period of time. The other aspect of confidentiality is the protection of traffic flow from analysis. This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility.

Non-Repudiation- Non-repudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

2.3 Generic AAA Architecture

Because of the significance of the AAA infrastructure and widespread popularity of the Internet and Multimedia services, special group within the IRTF (Internet Research Task Force) was created- AAArch Research Group- to continue research in the area of architectural development. This group ceased to exist in 2004; nonetheless some significant work has been carried out, including generation of RFC2903 “Generic AAA Architecture” [7]. It proposed an AAA infrastructure composed of generic AAA servers communicating via a standard protocol. The server activity is general; however, different applications requiring AAA services will have unique needs. Following components could be outlined:
- Application Specific Module (ASM) - ASMs are capable of handling even complex authentication and authorization requests. They interact with the generic server. The server will know to which ASM to forward a request and will receive an answer from the ASM whether the user is authenticated or not.
- Service Equipment (SE) - The SE provides a service to a user such as access to the internet.
- Authorization Event Log - This database is used to log the authorizations happening in the server. These events are used for accounting purposes. To account a user, the server has to know for example how long it used the authorized service. Authorization to a request can also be made depending on an event that occurred in the past.
- Policy Repository - This database contains the available services that can be authorized to a request.

The generic server interactions are shown in the Figure 1. The generic AAA server receives request, processes and forwards request to AAA server by means of common protocol. For the other interactions other protocols will be used.

![Diagram of Generic AAA Architecture](image)

Figure 1: Generic AAA Architecture

RFC2903 also stresses the importance of investigation of the management rules in the multi-domain AAA infrastructure because the future success is highly dependent on the manageability of this infrastructure.
Other work carried out by the AAAarch Research Group was concerned with Authorization Framework [8]. Based on the research of the group a memo was published containing Authorization Requirements [9]. The document outlines the main requirements for the creation of AAA protocol and provides separate guidelines under the following headings: security of authorization information, application proxying, trust models, administration etc.

In the next sections we look at some of the protocols that are actively being used in the AAA infrastructure. The examples of the older authentication protocols are PAP (PPP Authentication Protocol) [10] and CHAP (Challenge-handshake Authentication Protocols) [11]. These two protocols are commonly used in Point-to-Point communication links. In PAP the password is transmitted over without any protection which makes it vulnerable to the eavesdropping attacks. CHAP is a bit more secure and uses MD5 checksum hash to provide integrity during the three-way handshake authentication process. These protocols were commonly used in the wired connections; however, in the wireless environment, where more threats are present due to the open nature of communication, there is a common demand for better and more secure protocols.

### 2.4 Extensible Authentication Protocol (EAP) Framework

A number of Layer2 security protocols exist, but EAP [12] is probably one of the most commonly used. An interesting thing about EAP is that it is not really an authentication protocol, but rather a transport framework that supports a number of authentication mechanisms or methods. These methods can offer different levels of security. For example EAP-MD5 offers minimum level of security as it uses MD5 hashing algorithm that is considered weak and vulnerable to dictionary attacks. On the other hand EAP-TLS [13] is a strong method that uses PKI (Public Key Infrastructure). EAP-TLS is not commonly used in the wireless environment as public-key cryptography has a high level of overhead and demands more processing power that symmetric cryptographic methods.

The EAP framework is peer-to-peer and is based on request/response model. The format of EAP packet is shown in Figure 2:

<table>
<thead>
<tr>
<th>Code</th>
<th>Identifier</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data...</td>
<td></td>
</tr>
</tbody>
</table>

Figure 2: EAP Packet Format
Packet is 32 bit wide with Code field occupying 8 bits. There are only 4 codes defined for EAP: 1- Request, 2- Response, 3-Success, 4-Failure.

EAP can operate in pass-through mode when authenticator has to query the authentication server. In this case EAP peer sends request to the authenticator that in turn forwards query to the authentication server. In the diagram below an EAP Peer sends a request to the authentication server via Authenticator (Access Point or Network Access Server). EAP message is encapsulated into Point-to-Point Protocol (PPP), 802.1X or Protocol for carrying Authentication for Network Access (PANA) in the Peer-Authenticator transaction and over an AAA protocols between Authenticator and the Authentication Server.

IEEE 802.1X standard, also known as EAPOL (EAP over LAN), is aimed to provide authentication mechanism for port-based network access control that makes use of 802 LAN infrastructure by using EAP methods. In this case if a client using 802.11 wants to access Internet services it sends a request through Access Point that later forwards EAP message to AAA server over the LAN as shown in Figure 4.
2.5 Public Key Infrastructure X. 509 Certificates Framework

Public Key Infrastructure X.509 Certificates can be used in variety of applications that use web browsing, e-mail, user authentication services etc. The protocol outlined in RFC3280 [14] describes basic mechanism of operation. The protocol itself does not dictate use of a specific public key algorithm; however, its RFC document’s examples use RSA. Initially, user has to obtain a X.509 Certificate from a trusted Certificate Authority (CA). Below are listed fields included in the X.509 Certificate [6]:

- **Version**: Differentiates among successive versions of the certificate format; the default is version 1. If the Issuer Unique Identifier or Subject Unique Identifier is present, the value must be version 2. If one or more extensions are present, the version must be version 3.
- **Serial number**: An integer value, unique within the issuing CA, that is unambiguously associated with this certificate.
- **Signature algorithm identifier**: The algorithm used to sign the certificate, together with any associated parameters. Because this information is repeated in the Signature field at the end of the certificate, this field has little, if any, utility.
- **Issuer name**: name of the CA that created and signed this certificate.
- **Period of validity**: Consists of two dates: the first and last on which the certificate is valid.
- **Subject name**: The name of the user to whom this certificate refers. That is, this certificate certifies the public key of the subject who holds the corresponding private key.
- **Subject's public-key information**: The public key of the subject, plus an identifier of the algorithm for which this key is to be used, together with any associated parameters.
- Issuer unique identifier: An optional bit string field used to identify uniquely the issuing CA in the event the X.500 name has been reused for different entities.
- Subject unique identifier: An optional bit string field used to identify uniquely the subject in the event the X.500 name has been reused for different entities.
- Extensions: A set of one or more extension fields. Extensions were added in version 3 in order to enable addition of optional fields that may be deemed important by some organizations implementing security.
- Signature: Covers all of the other fields of the certificate; it contains the hash code of the other fields, encrypted with the CA's private key. This field includes the signature algorithm identifier.

Figure 5 shows the steps taken to sign user’s certificate. As can be seen from the diagram, the authenticity of user is provided by the CA. Also, no other party than CA can modify certificate without this being detected. In cases when the security has been compromised or validity period of the certificate has expired, it is responsibility of the corresponding CA to revoke this certificate.

![Figure 5: User Certificate signing](image)

### 2.5.1 Authentication Procedure

Authentication procedure that uses X.509 Certificates can be used in order to provide mutual authentication of the communicating parties. These includes 2-Way and 3-Way authentication. Figure 6 below shows steps and information necessary to accomplish the latter:
• First message is sent signed with A’s private key, includes timestamp, nonce generated by A, ID of the corresponding party and a session key encrypted with B’s public key
• B responds with a message containing its own timestamp and nonce, A’s ID, A’s nonce that was sent in the previous message and a matching session key encrypted with A’s public key
• The last steps is specific to 3-Way authentication and is only required in cases when synchronization clocks are not available

Furthermore it should be noted that when the procedure takes place in the real world there is an additional level of protection provided by the Transport Layer Security (TLS) [15] that handles transport of the authentication messages.

2.5.2 Implementation Issues

PKI X.509 infrastructure presents a fairly good security framework, nonetheless, there are issues related to the implementation of the infrastructure. One of the weaknesses comes from the fact that the framework does not impede implementation and utilization of weak security methods. For example, the use of previously widely accepted MD5 algorithm for hashing may produce security vulnerability due to the flaws in the algorithm’s design and its relative weakness. A whole range of issues surface related to specific vendor implementations. Infrastructure’s security model is based on the reliability and competence of the Certificate Authority. The question that might be posed is “who guards the guards” as some CAs might abuse trust through adoption of feeble practices. It is reported that often when X.509 Certificate expires, CA will renew subscription, but without the issue of new key-pair thus encouraging a prolonged key exposure. The root of the problem resides in the poor control of the service providing CAs [16].
2.6 Protocol for carrying Authentication for Network Access (PANA) Architecture

PANA [17] is a relatively new protocol that was created to enable to perform network-layer authentication independent of the underlying link-layer technology. PANA is a UDP-based EAP lower layer that runs between the EAP peer and the EAP authenticator (Figure 3). Since UDP (destination port 716) is used at the transport layer it is the responsibility of the protocol to retransmit lost or damaged messages, as UDP does not provide mechanisms for retransmission.

Figure 7 displays the main components of the architecture: PANA Client (PaC), PANA Authentication Agent (PAA), Enforcement Point (EP) and the Authentication Server.

- PANA Client (PaC): The PaC is the client implementation of PANA and resides on the node wishing to gain access to the network.
- PANA Authentication Agent (PAA): The PAA is the server implementation of PANA. It is the responsibility of PAA to interface with PaC in order to authenticate and authorize network access.
- Enforcement Point (EP): EP controls access to network resources. All the network traffic directed at PaC will have to pass through EP. The EP uses non-cryptographic and cryptographic filters to check data packets. In case if cryptographic access control is used, a security association needs to be established between EP and PaC. Once association is established per-packet security is enabled to provide integrity protection.
- Authentication Server (AS): Authentication Server makes decision on whether the end system can be authenticated or not. AAA protocol is used on the communication link between PAA and AS.

The following stages can be distinguished in the functioning of the protocol:
1. Authentication and authorization phase—once communication was started by either PAA or PaC, the actual exchange of EAP messages occurs. Once this phase is over PAA knows whether the PaC is authorized or not.
2. Access phase—during this stage PaC gains access to network and can send and receive IP traffic that passes through EP. It is also possible to send ping packets by PANA peer in order to verify that the session is still active.
3. Re-authentication—session can enter re-authentication stage, where current session’s lifetime is extended in case if re-authentication is satisfied. Otherwise session is terminated.
4. Session termination can be initiated by either of two parties: PaC or PAA.

PANA message codes have a general request/answer type of communication. The important data within the message is embedded in AVPs (Attribute-Value-Pairs). A protocol defines the following command codes:

- PANA-Client-Initiation (PCI)
- PANA-Auth-Request (PAR)
- PANA-Auth-Answer (PAA)
- PANA-Termination-Request (PTR)
- PANA-Termination-Answer (PTA)
- PANA-Notification-Request (PNR)
- PANA-Notification-Answer (PNA)

2.7 IP Multimedia Subsystem (IMS) Infrastructure

It is only logical that the next step in the development of telecommunication networks would be integration of the wireless services where users will see transition to the all-IP services. Some of the principle entities of the converged Next Generation Network (NGN) architecture include:

- Business Support Systems (BSS) that focus on management of business relationships with customer and include such tasks as billing, payment processing, revenue management etc.
- Operation Support Systems (OSS) provide support for network management including provisioning, troubleshooting, inventory.
- Service Delivery Platforms (SDP) support creation, deployment, execution and management of one or several classes of services. SDP also provides a managed 3rd party access to network services through web services standard.
- 3GPP IP Multimedia Subsystems (IMS) is an architectural framework for delivering IP multimedia services. The biggest achievement of IMS is decoupling of the application and control planes from the underlying access technologies.
With the current move to new 3G technology mobile operators commonly try to conform to the standards and interfaces specified by 3GPP/3GPP2. Both of these organizations are not privately owned bodies but rather associations of telecommunication groups that set as their main goal to define a number of technical specifications that later would be globally applicable in the telecommunication industry. 3GPP (3rd Generation Partnership Project) defines technical specification for technologies that have evolved from the GSM technology. A number of task groups exist within 3GPP each one charged with specific architecture-related development tasks.

Another organization that executes similar tasks is 3GPP2. This organization is charged with development of technical specifications for 3rd Generation network devices that are based on the Code Division Multiple Access (CDMA) access technology that is very widely deployed in the North America and Japan.

Deployment of 3G networks heralds creation of improved telecommunication infrastructure. Arrival of IMS (IP Multimedia Subsystem) was a major step taken for the provision of IP Multimedia services to the users of mobile networks. IMS is a subsystem of 3GPP; its equivalent in 3GPP2 is called the MultiMedia Domain (MMD). Both frameworks perform the same function i.e. provide access to IP multimedia services to mobile users and share similar architectural design. As far as the project is concerned, we are primarily interested in the signalling interfaces and functional entities related to the AAA functionality. Thus we will take a closer look at what functional elements the 3P-AAA framework could inherit from the 3GPP IMS architecture.

2.7.1 IMS Architectural Overview

The primary entities of the diagram describe architectural layout of the IMS. As can be seen in Figure 8, 3GPP separates Transport and IMS planes from the Service plane. This creates a level of abstraction that permits development of the new services independent from the lower levels.

- CSCF (Call Session Control Function) - this entity can be of four different types: Proxy, Interrogating, Emergency and Serving. CSCF can be seen as an intermediary body in communication between the mobile user and the Home Subscriber Server (HSS). When User Equipment (UE) first tries to access IMS Proxy CSCF (P-CSCF) is responsible for finding and associating this user and Serving CSCF. P-CSCF sits on the pass of all signalling messages and can inspect every message. Another important function carried out by this entity is authentication of the UE. Additionally, it is responsible for generation of charging records. Interrogating CSCF (I-CSCF) is primarily used for roaming scenarios as it is responsible for locating the corresponding HSS for the subscriber in question. Emergency CSCF (E-CSCF) shall be able to retrieve geographical location information from the Location Retrieval
Function (LRF) in the case that the geographical location information is not available and is required [18]. Serving CSCF (S-CSCF) is the central entity of the signalling plane and is typically located within the home network. It is also an enforcement point of the network.

- **HSS (Home Subscriber Server)** - a central piece in this architecture as it can be seen as a master database. This database stores user identity information, all the security vectors, network access information and user profile information. HSS is responsible for generation of information that is used for user authentication and integrity checks. Other entities such as AuC (Authentication Centre), EIR (Equipment Identity Register) and HLR (Home Location Registered) logically would reside within HSS.

- **AS (Application Server)** – support for three different types of application servers are provisioned within the framework: Session Initiation Protocol (SIP) Application server, Open Service Access (OSA) Application server and Customer Application for Mobile network Enhanced Logic (CAMEL) IP Multimedia Service Switching Function (IM-SSF) server. These servers offer value-added services and can reside either inside the network or in the 3rd party location. Application servers interact with S-CSCF using SIP protocol. In case if the SIP Application server resides within the home network, it can access HSS directly through Sh Diameter interface. One peculiarity of the OSA Application server is that it does not interact directly with IMS but does so through OSA Server Capability Server. IM-SSF provides transition for legacy services.

Figure 8: IMS Architecture
Two signalling protocols can be emphasized from the given architectural outline: SIP and Diameter. Operations related to the policy control, subscriber information access, charging and billing are handled by the 3GPP-extended Diameter protocol. User-interaction session control and application service interactions are handled by SIP. The Third-party Value Added Service Provider (VASP) communicates with the underlying network by means of OSA/Parlay interface. Creation of the OSA API is a joint effort between ETSI (European Telecommunication Standardization Institute), 3GPP and The Parlay Group [19].

2.8 Session Initiation Protocol Framework

Session Initiation Protocol (SIP) is an application layer protocol used for session set up and control. It has been defined by RFC3261 [20]. This application level protocol that in structure resembles that of Hyper Text Transfer Protocol (HTTP) is currently widely deployed in a number of applications. As outlined in the specification document, SIP provides the following set of services:

- User location: determination of the end system to be used for communication;
- User availability: determination of the willingness of the called party to engage in communications;
- User capabilities: determination of the media and media parameters to be used;
- Session setup: "ringing", establishment of session parameters at both called and calling party;
- Session management: including transfer and termination sessions, modifying session parameters, and invoking services.

It can run on top of User Datagram Protocol (UDP) and Transmission Control Protocol (TCP), as well as newer Stream Control Transport Protocol (SCTP). The basic operation of the SIP can be described by the discovery and session setup between different network entities as well as negotiation of the session parameters. SIP is commonly used for control of multimedia streams. It uses Session Description Protocol (SDP) [21] to set up a multimedia session by listing session requirements. This mechanism can be used for provision of the appropriate QoS levels.

This type-text protocol uses a set of request/response messages to communicate between different entities of the infrastructure. The common requests are:

- REGISTER: Used by a User Agent to indicate its current IP address and the URLs for which it would like to receive calls.
- INVITE: Used to establish a media session between user agents.
- ACK: Confirms reliable message exchanges.
- CANCEL: Terminates a pending request.
- **BYE**: Terminates a session between two users in a conference.
- **OPTIONS**: Requests information about the capabilities of a caller, without setting up a call.
- **PRACK (Provisional Response Acknowledgement)**: PRACK improves network reliability by adding an acknowledgement system to the provisional Responses (1xx). PRACK is sent in response to provisional response (1xx).

Figure 9 below shows an example of the session setup between two SIP User Agents. The session is torn down once media transfer is finished. As can be seen from the diagram, the response format is similar to the HTTP response format:

- **Provisional (1xx)**: Request received and being processed.
- **Success (2xx)**: The action was successfully received, understood, and accepted.
- **Redirection (3xx)**: Further action needs to be taken (typically by sender) to complete the request.
- **Client Error (4xx)**: The request contains bad syntax or cannot be fulfilled at the server.
- **Server Error (5xx)**: The server failed to fulfill an apparently valid request.
- **Global Failure (6xx)**: The request cannot be fulfilled at any server.

![Figure 9: SIP Call Session](image)

SIP inherited some of its authentication methods from HTTP. However, this Digest Access Authentication method only allows the server to authenticate the user but
does not support the reverse operation of authenticating the server to the user. Since SIP is so widely spread, a number of security extensions were developed for it. Typically an X.509 Certificate exchange takes place during TLS setup that requires use of TCP; however, there is an extension that allows an X.509 Certificate exchange over SCTP [22]. That means that X.509 Certificate based authentication may be performed to mutually authenticate the Mobile User and the access network element.

An additional functionality of SIP is that it can provide location management and presence related services. This ability is especially valuable in the modern environment where user may have several communication devices.

2.9 Conclusion

The principle goal of this chapter was to make an introduction to the technical aspects related to the AAA framework. Going from the general to the specific, the security services and the generic AAA architecture were discussed first followed by the more specific description of the EAP and the X.509 Certificates. The X.509 Certificates are discussed in a greater detail, since the certificate exchange mechanism is quiet suitable for the implementation of the mutual authentication within the 3P-AAA framework. The signalling protocols were introduced in order to see what features can be inherited by the 3P-AAA signalling protocol. Since PANA was design specifically for the provision of the authentication features, these features could be integrated into the 3P-AAA signalling. On the other hand, SIP provides a wider array of session control services, including the authentication, and is more suitable for handling the multimedia sessions. As a matter of fact, SIP and Diameter, which will be discussed in the next chapter, are the two primary signalling protocols employed by the IMS framework. Finally, in order to see how some of the technical aspects and features can be combined together, IMS was presented as a real world example of a functional framework.
CHAPTER 3

AAA PROTOCOLS- RADIUS AND DIAMETER

3.1 Introduction
The authentication protocols looked at in the previous chapter carry out Authentication/Authorization functions however they do not monitor the usage of network resources. Implementation of the “true” AAA protocol should not only perform Authentication and Authorization, but also Accounting where careful records of the network/service consumptions should be taken. This chapter focuses on two widely used AAA protocols: RADIUS and its descendant Diameter. Both of these protocols provide the AAA functionality, however, Diameter is newer and was developed to overcome the weaknesses of its predecessor and thus will be discussed in greater detail. With the introduction of the Diameter Base protocol a number of supporting applications has emerged to provide additional functionality and supporting features. The principle purpose of this chapter is to demonstrate that the rich set of features provided by the Diameter protocol would allow it to become the foundation of the 3P-AAA signalling.

3.2 Remote Authentication Dial-In User Service (RADIUS)

RADIUS [23] protocol is a true AAA protocol as it is concerned with Authentication, Authorization and Accounting features. RADIUS is very commonly used by Internet Service Providers (ISPs) to manage access to network resources. One of the disadvantages of RADIUS is its poor scalability as it does not provide any congestion control mechanisms.

RADIUS uses client-server model of communication. A Network Access Server (NAS) acts as a client of RADIUS. It contacts the RADIUS server. In order to improve the scalability issue RADIUS server network can be organized in the hierarchical manner, where in case if the authorization request cannot be resolved at the local RADIUS server, the request will be forwarded to the next server up the hierarchy chain. When client wishes to authenticate using RADIUS, it creates an “Access-Request” with such attributes as user’s name, password, ID of the client etc. In order to provide integrity of the message the password is hidden using the RSA MD5.
Once the RADIUS server receives the request, it validates the sending client. A request from a client for which the RADIUS server does not have a shared secret must be silently discarded. If the client is valid, the RADIUS server consults a database of users to find the user whose name matches the request. The user entry in the database contains a list of requirements which must be met to allow access for the user. This always includes verification of the password, but can also specify the client(s) or port(s) to which the user is allowed access.

The server might challenge the client. In this Access-Challenge response a pseudorandom number, also known as nonce will be send. Using the pre-shared key client will encrypt the number and return it to the server. RADIUS uses UDP for transport and two ports have been assigned to the RADIUS protocol: 1812 for RADIUS Authentication and port 1813 for RADIUS Accounting. However, prior to the official assignment of port by the IANA (the Internet Assigned Number Authority), ports 1645 and 1646 were used. These ports are still in use for backward compatibility. Designers of the protocol considered that UDP was a better option for AAA as it provided less overhead and simplified the server implementation due to the stateless nature of the protocol.

As well as that, in comparison to PANA, where keep-alive messages are being exchanged in order to verify that the session is still active, RADIUS discourages the use of keep-alive messages since they don’t provide any additional useful information. It is suggested that other protocols, such as Simple Network Management Protocol (SNMP) should be used for these purposes.

Because RADIUS uses MD5 hashing that is considered to be cryptographically weak [24], it is recommended to use other security protocols such as IPsec [25, 26] or TLS [15].

### 3.2.1 RADIUS Message Format

As seen in Figure 10, the message is 32bit wide. The following codes are identified in the authentication protocol:

- 1 Access-Request
- 2 Access-Accept
- 3 Access-Reject
- 4 Accounting-Request
- 5 Accounting-Response
- 11 Access-Challenge
- 12 Status-Server(experimental)
- 13 Status-Client(experimental)
- 255 Reserved
The identifier field is only one octet and is used to match requests and responses. In addition each message can carry a number of attributes that relate information between the client and the server.

![RADIUS Message Format](image)

**Figure 10: RADIUS Message Format**

### 3.2.2 RADIUS Accounting

When a client is configured to use RADIUS Accounting, at the start of service delivery it will generate an Accounting Start message describing the type of service being delivered and the user it is being delivered to, and will send that to the RADIUS Accounting server, which will send back an acknowledgement that the message has been received. At the end of service delivery the client will generate an Accounting Stop message describing the type of service that was delivered and optionally statistics such as elapsed time, input and output octets, or input and output messages. It will send that to the RADIUS Accounting server, which will send back an acknowledgement that the message has been received.

It is recommended that the client continue attempting to send the Accounting-Request packet until it receives an acknowledgement, using some form of back off algorithm. If no response is returned within a length of time, the request is resent a number of times. The client can also forward requests to an alternate server or servers in the event that the primary server is down or unreachable. An alternate server can be used either after a number of tries to the primary server fail, or in a round-robin fashion. If the RADIUS accounting server is unable to successfully record the accounting packet it must not send an Accounting-Response acknowledgment to the client.

The format of the messages for RADIUS accounting is the same as for authentication where Attributes would be specifically defined for accounting purposes.
### 3.3 Diameter

RADIUS is a very popular protocol and is widely used by the operators. However, due to some shortcomings of the RADIUS original design and overall changes in the requirements due to the development in telecommunication industry, a better and more reliable protocol was needed. Therefore it is envisaged that the newly developed AAA Diameter [27] protocol will replace RADIUS in the near future.

The Diameter base protocol provides the minimum requirements needed for an AAA protocol as described in [28]. The base protocol may be used by itself for accounting purposes only, or it may be used with other Diameter application.

There are a number of reasons why Diameter is seen as the successor of RADIUS, the major one being a more careful design and consideration for future development. Diameter was designed to be extensible. Extensibility can be achieved through addition of new application specific command codes and Attribute Value Pairs (AVPs). Among other advantages of Diameter, the following may be listed:

- Diameter provides more reliable transport by running over TCP and SCTP, in comparison to UDP transport of RADIUS.
- Unlike RADIUS which does not describe any failover mechanism, Diameter defines failover algorithms and the corresponding state machine.
- As far as transport-layer security is concerned, it’s a requirement for Diameter applications to support IPsec or TLS.
- Diameter base protocol provides agent support, thus a Diameter peer can be a Redirect, Proxy or Relay agent.
- Diameter possesses better roaming support. Even though the concept of proxying exists in RADIUS, due to poor transportation security and lack of auditability, it is vulnerable to the man-in-the-middle attacks. Diameter with its features allows for better roaming and scalability.
- Diameter supports error handling and capacity negotiations

Diameter is designed as a peer-to-peer architecture, and a Diameter node can act as a client or as a server depending on the network implementation. Apart from the Redirect, Proxy and Relay agents, Translation agent is supported by the Diameter protocol to provide backward compatibility with RADIUS.

The base Diameter protocol concerns itself with capabilities negotiation, how messages are sent and how peers may eventually be abandoned. The base protocol also defines certain rules that apply to all exchanges of messages between Diameter nodes.

Communication between Diameter peers begins with one peer sending a message to another Diameter peer. The set of AVPs included in the message is determined by a
particular Diameter application. One AVP that is included to reference a user's session is the Session-Id.

The initial request for authentication and/or authorization of a user would include the Session-Id. The Session-Id is then used in all subsequent messages to identify the user's session. The communicating party may accept the request, or reject it by returning an answer message with the Result-Code AVP set to indicate an error occurred. The specific behaviour of the Diameter server or client receiving a request depends on the Diameter application employed.

The session state (associated with a Session-Id) must be freed upon receipt of the Session-Termination-Request, Session-Termination-Answer, expiration of authorized service time in the Session-Timeout AVP, and according to rules established in a particular Diameter application.

Diameter base protocol support both TCP and SCTP transport protocols and is allocated port 3868. It is specified in the base protocols that while client can support either of the two transport methods, the agents and the servers must support both.

### 3.3.1 Diameter nodes and agents

The typical entries within the protocol are clients and servers, however for scalability and backward compatibility other nodes were introduced into the system: relay agents, proxy agent, redirection agent and translation agent.

- **Relay Agents** - Relays forward requests and responses based on routing-related AVPs and realm routing table entries. Figure 11 demonstrates basic use of a relay agent. Since relays do not make policy decisions, they do not examine or alter non-routing AVPs. As a result, relays never originate messages, do not need to understand the semantics of messages or non-routing AVPs, and are capable of handling any Diameter application or message type. Since relays make decisions based on information in routing AVPs and realm forwarding tables they do not keep state on NAS resource usage or sessions in progress.

![Figure 11: Diameter Relay Agent](image-url)
• Proxy Agents – Similar to relays, proxies forward request and response messages and their operational diagram is equal to that of Figure 11. However, proxies also make policy decisions related to resource usage and provisioning. This is typically accomplished by tracking the state of NAS devices. While proxies typically do not respond to client Requests prior to receiving a Response from the server, they may originate Reject messages in cases where policies are violated. As a result, proxies need to understand the semantics of the messages passing through them, and may not support all Diameter applications.

• Redirection Agents - Rather than forwarding requests and responses between clients and servers, redirect agents refer clients to servers and allow them to communicate directly (Figure 12). Since redirect agents do not sit in the forwarding path, they do not alter any AVPs transiting between client and server. Redirect agents do not originate messages and are capable of handling any message type, although they may be configured only to redirect messages of certain types, while acting as relay or proxy agents for other types. As with proxy agents, redirect agents do not keep state with respect to sessions or NAS resources.

Figure 12: Diameter Redirect Agent
Translation Agents - A translation agent is a stateful Diameter node that is used to provide backward compatibility with legacy protocols. It performs protocol translation between Diameter and another AAA protocol, such as RADIUS (Figure 13).

![Figure 13: Diameter Translation Agent](image)

### 3.3.2 Diameter Messages

All the information between different Diameter nodes is exchanged by means of messages that have specific structure. The outline of the Diameter header is given in Figure 14. Each message carries command code that specifies the action that peer is currently performing, but the real data is carried by the AVPs of the message.

![Figure 14: Diameter Header](image)

Command Flags filed is 8 bit wide. Only the first four bits are assigned in the base protocol. These are Request, Proxiable, Error and Potentially Retransmitted Message bits. It must be noted that if the Request bit is set, i.e. message is a request message then the Error bit must be cleared.

Hop-by-Hop Identifier field is used for matching request and reply messages. End-to-End Identifier is used to detect duplicate messages in case of failover.
In the Diameter base protocol 14 command code messages were defined listed in Table I:

Table I: Base Diameter message codes

<table>
<thead>
<tr>
<th>Message Name</th>
<th>Abbreviation</th>
<th>Command Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abort-Session-Request</td>
<td>ASR</td>
<td>274</td>
</tr>
<tr>
<td>Abort-Session-Answer</td>
<td>ASA</td>
<td>274</td>
</tr>
<tr>
<td>Accounting-Request</td>
<td>ACR</td>
<td>271</td>
</tr>
<tr>
<td>Accounting-Answer</td>
<td>ACA</td>
<td>271</td>
</tr>
<tr>
<td>Capabilities-Exchanging-Request</td>
<td>CER</td>
<td>257</td>
</tr>
<tr>
<td>Capabilities-Exchanging-Answer</td>
<td>CEA</td>
<td>257</td>
</tr>
<tr>
<td>Device-Watchdog-Request</td>
<td>DWR</td>
<td>280</td>
</tr>
<tr>
<td>Device-Watchdog-Answer</td>
<td>DWA</td>
<td>280</td>
</tr>
<tr>
<td>Disconnect-Peer-Request</td>
<td>DPR</td>
<td>202</td>
</tr>
<tr>
<td>Disconnect-Peer-Answer</td>
<td>DPA</td>
<td>202</td>
</tr>
<tr>
<td>Re-Auth-Request</td>
<td>RAR</td>
<td>258</td>
</tr>
<tr>
<td>Re-Auth-Answer</td>
<td>RAA</td>
<td>258</td>
</tr>
<tr>
<td>Session-Termination-Request</td>
<td>STR</td>
<td>275</td>
</tr>
<tr>
<td>Session-Termination-Answer</td>
<td>STA</td>
<td>275</td>
</tr>
</tbody>
</table>

As well as that, the Diameter Base protocol defines a number of AVPs that would be quite common in the AAA type of application. It can be said that it is AVPs that carry the “real” data in the given protocol.

Each AVP has an AVP code that can be found in the AVP header (Figure 15), which uniquely identifies it. AVP numbers from 1 to 255 are reserved for backward compatibility with RADIUS.

AVP Flags provide additional information on how attributes must be handled. The ‘r’ bits should be set to 0 and are reserved for future applications. The ‘P’ bit indicates need for end-to-end security.
‘M’ bit stands for Mandatory and all Diameter implementations are required to support these AVPs. AVPs with this bit cleared are informational.

‘V’ bit is a Vendor-Specific bit and indicates whether the optional Vendor-ID is present.

Apart from the Basic Data formats, such as OcterString, Integer and Float, AVPs can support derived data formats. It is also allowed to use AVP values of type ‘Grouped’ where Data field is a sequence of AVPs. This allows for AVP nesting, when one Grouped AVP contains another Grouped AVP within.

### 3.3.3 Diameter Peers

Even though a Diameter node can have multiple peer connections sometimes it is not economical to establish connection to all of them. At a minimum Diameter node must have an established connection with two peers per realm, these peers are called primary and secondary peer. Secondary peer is used in case if the connection with primary peer has failed. Additional connections can be established if the need for them arises.

An important enhancement of Diameter is its peer discovery capabilities. Before a connection can be established between peers, they must exchange the Capabilities Exchange messages. In case if no common applications or common security was discovered, the peers should disconnect transport layer connection. It is also important to note that CER and CEA messages must not be proxied, redirected or relayed.

Given the nature of the Diameter protocol, it is recommended that the transport failures be detected as soon as possible. Detecting such failures will minimize the occurrence of messages sent to unavailable agents, resulting in unnecessary delays, and will provide better failover performance. The Device-Watchdog-Request and Device-Watchdog-Answer messages are used to proactively detect transport failures.

The communication between peers in Diameter follows a specific State Machine described in section 5.6 of [27]. This State Machine is used to open, close, failover, probe, and reopen transport connections. The watchdog messages are used to verify that the connection is still active.

### 3.3.4 Error Handling

Errors that occur in the Diameter fall into two categories: protocol and application errors. Protocol errors occur at the base protocol level. On the other hand application
errors generally occur due to the problems associated with a function of the specific Diameter application.

Result-Code AVP values that are used to report protocol errors must only be present in answer messages where ‘E’ bit is set. Typically Result-Code AVP describes the error that the Diameter node encountered and can be used for debugging purposes.

Error code of Diameter is similar to the semantics of the HTTP protocol. The first digit of the return code will identify the type of error:

- 1xxx Informational
- 2xxx Success
- 3xxx Protocol Errors
- 4xxx Transient Failures
- 5xxx Permanent Failures

Only the errors that fall into Protocol Errors category should have ‘E’ bit set in the answer message. The difference between Transient and Permanent Failures is that the former signifies that the request could not be satisfied at this time, but may be successful in the future, while the latter signifies that the request should not be attempted again.

### 3.3.5 Diameter Sessions

The Diameter Base protocol can provide two types of services to applications. First type involves the authentication and the authorization, and can optionally make use of the accounting. Second only makes use of the accounting.

When authentication and/or authorization takes place, a user sends request to the server. This request contains a Session-Id AVP. All subsequent messages that belong to the same session must contain this matching Session-Id AVP.

Because authentication/authorization messages are largely application specific, the authorization requests are not included in the base protocol. However, base protocol defines messages that are used for session termination. Session termination messages can be initiated by either Diameter client or server. Session-Termination-Request or Abort-Session-Request commands will be used in this case. When application makes use of only Accounting services, the Session-Id AVP still would be used, however, session termination will be signalled by issuing an accounting stop message.

Base protocol contains a set of finite state machines that must be observed by all Diameter implementations. Separate state machines exist for Authorization and Accounting services. There are four different authorization session state machines supported in the Diameter base protocol. The first two describe a session in which the server is maintaining session state, indicated by the value of the Auth-Session-State AVP (or its absence). One describes the session from a client perspective, the
other from a server perspective. The second two state machines are used when the server is stateless. Here again, one describes the session from a client perspective, the other from a server perspective.

### 3.3.6 Accounting

The Diameter Accounting protocol is based on a server directed model with capabilities for real-time delivery of accounting information. The server directed model means that the device generating the accounting data gets information from either the authorization server (if contacted) or the accounting server regarding the way accounting data shall be forwarded. Several fault resilience methods have been built in to the protocol in order minimize loss of accounting data in various fault situations and under different assumptions about the capabilities of the used devices. Due to the purpose of the accounting protocol a real-time transfer of data is a requirement, it needs to be fulfilled in order to perform credit limits checks.

Some of Diameter mechanisms are used to overcome small message loss and temporarily network failures. It is a requirement for a Diameter client to implement failover mechanism described in the base protocol. It is also recommended to use non-volatile storage for accounting records until the acknowledgment from the Diameter server was received. This mechanism can be used when network congestion cause delays or when Diameter server is temporarily down.

Base protocol has four types of accounting message AVPs: EVENT_RECORD, STOP_RECORD, START_RECORD and INTERIM_RECORD. INTERIM_RECORD may be used in cases when client accesses services for a lengthy period of time, where timing interval can be set and may also depend on Re-Authorization and Re-Authentication timer. EVENT_RECORD indicates one-time event (event where start and stop occur simultaneously) and carry all the relevant information. Since it is possible for one client to access multiple services within one session, the Diameter messages must contain AVPs that use the same session-ID but will use different sub session-IDs.

### 3.3.7 Diameter Credit Control

Since the time of the development of the original protocol, a number of other applications were implemented using Diameter protocol targeting specific services, such as Diameter SIP Application for session management, Diameter EAP Application implementing EAP framework, Diameter Credit Control Application [29] etc. Credit Control application’s significance is that it enables the service provider to implement online real-time charging with credit reservation. Many interface used in 3GPP for charging and billing use Credit Control Application [30]. In comparison to the base protocol Credit Control Application only defines two
new messages. These messages are Credit Control Request and Answer. Since the signalling strength of the protocol rests with the data encoded in AVPs, this application defines a great number of new AVPs specific to the credit control task.

The application differentiates between two distinct modes of charging: session based and one-time events. Session based charging performs multiple interrogations of the Credit Control server during an on-going session. Since some scenarios may include possibility of access of multiple services per user session, sub-session charging is also facilitated. One-time event was created to accommodate request that do not require multiple interrogations and could be satisfied by a single request/answer message. These scenarios include direct debiting, credit checks and price enquiries.

### 3.3.8 Diameter’s Evolution

Diameter was created to serve as a successor to RADIUS. There are plenty of examples of wide adaptation of this protocol in the industry. Regardless of the careful architectural design and wide spread adoption, some issues have surfaced only during implementation and deployment of the protocol. Evolving standards have created different interpretations and implementation that lead to incompatibilities between vendors [31].

Some flaws have been found related to the protocol design. For example, the initial information exchange between peers that helps to establish a connection is not clearly specified in the RFC3588 and its interpretation may only be deduced from the state machines. The establishment of communication will be influenced by the list of the supported vendor identifiers. The problem here emerges when the corresponding end-to-end nodes support the same list of vendor but the intermediary nodes participating in the routing do not.

A lot of problems encountered are due to inappropriate setting of the M(andatory)-flag. This flag is used inside AVP to state that this AVP has to be supported by the receiving node. Generally, there is confusion between the ABNF defining the set of AVPs used in a Diameter command for the particular Diameter Application and the setting of the M-bit of an AVP for this same application.

Based on the protocol deployment experiences and in order to solve interoperability issues, Diameter Maintenance and Extensions (DIME) Technical Working group came up with new version of protocol that is currently under discussion. RFC3588bis document claims full backward compatibility with the original RFC3588 [32]. Here are some of the principle changes outlined within RFC3588bis:

- Deprecated the use of Inband-Security AVP for negotiating transport level security. New version of Diameter will establish TLS on the well-known secure port prior to exchange of traffic.
- Deprecated the exchange of CER/CEA messages in the open state. It is assumed that the capabilities exchange in the open state will be described in more detail in a separate specification.
- Simplified security requirements. Use of secure transport is still mandatory; however, TLS will become the primary method of security traffic with IPsec being a secondary alternative. The support for end-to-end security framework has also been deprecated.
- The restriction concerning the support of accounting for all Diameter application is removed, as it does not make sense for some applications.
- Other small fixes address removal of obsolete types, fixes to command ABNFs, fixes to the state machine etc.
- Routing fixes are made through specification of what information can be used for making general routing decision. A separate internet draft is dedicated to Diameter routing optimizations [33].

3.4 Conclusion

This chapter has looked at the two principal AAA signalling protocols currently employed in the industry. Even though both protocols provide similar functionality, Diameter has more advanced features which make it more suitable and reliable for the purposes of this thesis. Also, Diameter was designed to be extensible and a number of new Diameter based applications has emerged after deployment of the Base protocol. These include Accounting and Credit Control applications that could be used to provide the offline and the online charging. Apart from the growing amount of the Diameter based applications, the Base protocol itself evolves and is currently going through a revision, aimed to remove some of the ambiguities and the original design flaws. Since the behaviour expected from the 3P-AAA signalling protocol introduces new features and scenarios that are not catered for in the original Diameter Base protocol, the Diameter 3P-AAA signalling protocol would have to define new messages and attributes in order to facilitate these salient features.
CHAPTER 4

3P-AAA FRAMEWORK

4.1 Introduction

As has been mentioned previously, the design of the 3P-AAA framework is one of the central issues in the development of the UCWW. This framework is conceived on the idea that the 3P-AAA service providers would be responsible for management and maintenance of the AAA features which would be separated from the provision of the access- and tele- services. The communication between different parts of the framework will take place through the new interfaces. The principle challenge is not only the through design of these interfaces but also their standardization. Overcoming the challenge of global standardization of the 3P-AAA interfaces would give a strong incentive to further development of the open 3P-AAA infrastructure. Due to the resilience requirements and sensitivity of the data traversing these interfaces, a careful examination of each interface’s functionality should be performed. The challenge is that the creation of 3P-AAA would produce new forms of interactions and scenarios that have not been previously seen. For example, regarding the decoupling of provision of teleservices from that of access communication services, the interaction with third-party VASP should be direct through one of these interfaces. This is quite different from the way third-party VASP services are being accessed now, i.e. through home access network where a Service Level Agreement (SLA) exists between home network and third-party VASP. Thus, prior to the actual service deployment, VASP has to be plugged into IMS Open Service Access (OSA) or other Service Delivery Platform. The principle tasks of these entities is that they perform accounting and charging tasks, and provide information regarding the network resources that can be accessed by the third-party VASP. Within 3P-AAA these entities can be replaced by interface interactions since charging and accounting will be serviced by the 3P-AAA service providers and network resources access can be advertised through other entities of UCWW i.e. Wireless Broadband Channels (WBC) and Advertisement, Discovery and Associations (ADA) agents [34].

This chapter sets out to cover the principle ideas outlined by the 3P-AAA framework. Sections that follow will outline the main entities and interfaces envisioned. In order to gather requirements for the 3P-AAA signalling, different forms of interactions between the 3P-AAA entities will be described in the section
covering signalling scenarios. This section covers a lot of material and looks at the interactions that take place during different stages of the access. Scenarios involving the 3P-AAA specific Hot Access-network Change (HAC) handover will look at the cases when more than one service provider is available in the area. Some of the novel forms of interactions that would be possible in the 3P-AAA environment are also outlined. The final section of this chapter will outline the possibility of the co-existence of the 3P-AAA with other technologies such as 3GPP IMS.

4.2 Entities

Figure 16 [35] shows the three principle interfaces envisioned for the 3P-AAA framework along with the principle functional elements of the framework.

- Mobile User (MU) - this entity is the typical end-consumer of the services provided by the other entities of the framework. MU will receive great flexibility and wider range of services through exchange of subscriptions with Internet Service Providers, Mobile Operators etc. for subscription with a third-party AAA provider. MU is an abstraction for generic user and can physically be represented by mobile phones, laptops or in some scenarios described later as another service provider.

- Access Network Provider (ANP) - 3P-AAA aims at separating provision of access from the provision of services. This entity represented as an ANP domain in the diagram, can be composed of numerous physical servers. Typically it would have an access server that would perform authentication and authorization and would be the first point of contact with a user. Since during provision of access, media and control stream will be flowing through this entity, it will perform policy enforcement and metering functions. ANP will also have a back-end server that would be connected to the 3P-AAA-SP
for the purposes of communication of the relative data. When offline charging is involved, it may not be necessary to contact 3P-AAA server during authentication and authorization stage, hence, back-end server may handle these decisions based on the authentication procedure results.

- TeleService Provider (TSP) - this entity is responsible for the provision of non-access services. Just as ANP it would be composed of an access server and a back-end server connected to the 3P-AAA service provider. During provision of a teleservice, there is a certain dependence on the state of the session between MU and ANP, since transport is required for the service provision. This state will be monitored by the signalling interfaces.

- Value Added Service Provider (VASP) - this entity is responsible for the provision of value-added services. In telecommunication industry, Value Added Services (VAS) term encompasses a wide range of services and may be defined as any type of a non-core service available to the end user. Since provision of phone calls can be considered as a primary core service, VAS includes such commonly used mobile technologies as SMS, MMS and GPRS. Currently most of the VAS are implemented and deployed by the mobile operators. As a result, in order to gain access to some VAS and applications, a mobile user first needs to create a service level agreement with a mobile operator.

- 3P-AAA-SP- this entity is the key element of the infrastructure. It is the vertex of the infrastructure’s communication charged with multiple critical tasks. The 3P-AAA-SP’s infrastructure must be secure, reliable and scalable. Hierarchic deployment of 3P-AAA servers could be a good strategy for the provision of scalability.

4.3 3P-AAA Interfaces

4.3.1 Interface ‘a’

This interface is responsible for the MU’s communication with the service providing entities, i.e. ANPs, TSPs, and VASPs. It is over this interface where a session with the service of interest is established and maintained. The aliveness of the session is monitored by the signalling messages. In case of events that might cause change in the session state, an informative update message is exchanged between communicating peers. When the mobile user has finished using the service, a session termination procedure would take place.

Security is a major concern for this interface, since it operates in the most vulnerable (i.e. wireless) environment in comparison to the other interfaces. Previously, as in Global System for Mobile Communication (GSM) networks, the authentication procedure between the mobile user and the network provider has been one-way only. However, nowadays wireless service providers can be easily spoofed
by malicious attackers. Taking this fact into consideration, it is important to perform a two-way authentication between communicating parties. 3P-AAA employs X.509 certificates for mutual authentication of peers. In order to provide strong authentication features, the three-way authentication option of X.509 should be employed. The benefit of the three-way authentication is that it puts less stringent requirements for time synchronization between different devices employed. In the 3P-AAA framework, the last (third) message carries also an authentication decision back to the party that initiated the authentication procedure.

4.3.2 Interface ‘b’

The primary purpose for this interface is to enable interaction between the mobile user and his/her 3P-AAA-SP. A number of diverse tasks can be attributed to this interface. The mobile user would be able to interact with his/her 3P-AAA account for purposes like checking the accounting information and possible profile settings interaction. Another key feature of the 3P-AAA framework is to provide accounting and billing transparency. Interacting with a multiple set of access- and teleservice providers, the mobile user has to be ensured that the charges applied by these diverse entities are indeed accurate. After each session termination procedure taking place, the mobile user issues a request to 3P-AAA-SP for Charging Detail Record (CDR) for the recently terminated session. The MU’s equipment can aggregate appropriate CDR information and calculate whether the charges applied have been accurate. In some scenarios where connection to the 3P-AAA-SP has been lost during an on-going session, it might be appropriate for the service provider to store accounting data locally without service interruption and later forward updated data to the 3P-AAA server. Even in this case, the state machine has to ensure that the CDR data is still delivered to the end user.

4.3.3 Interface ‘c’

This interface performs vital task of providing important information for authorization, accounting and charging tasks. All entities of the 3P-AAA framework that provide services would be connected by means of ‘c’ interface to the 3P-AAA-SP server. Security is also an important issue for this interface but unlike interface ‘a’, entities communicating by means of interface ‘c’ share security association through initial subscription. Resilience of the interface is of paramount significance since it handles accounting and charging related streams of data. Thus it should be able to handle failover scenarios. This interface will also provide a flexible charging to the framework through adaptation of the online and offline charging capabilities. Online charging is synonymous to the idea of the prepaid services, where in order to access services first a credit check is performed on the user account and certain amount is debited or reserved. Online charging is performed in real-time and can
thus influence the session state. Offline charging is less stringent and does not require the credit control facilities. When offline charging is used the usage of resource is reported and charges are applied based on the amount of resources consumed. This kind of charging is less flexible and is typically used for the subscription-based services.

4.4 3P-AAA Scenarios

This section will look at some signalling scenarios employed in the 3P-AAA framework. Based on this scenarios and requirements for the interfaces, signalling protocol details will be drawn up. Scenarios outlined here may be decomposed into three primary categories: those not involving handover procedures, scenarios with Hot Access network Change (HAC) and some novel scenarios that could be facilitated by the 3P-AAA infrastructure.

4.4.1 Basic Signalling Scenarios

Figure 17 shows a typical scenario where Mobile User accesses some ANP/TSP/VASP resources. These interactions can be broken into three principle phases:

1) Initial phase- mutual authentication using the X.509 Certificates takes place followed by the authorization performed to ensure that the Mobile User has clearance to access requested services.

2) Access phase- access and use of resources. Prior to granting access, the availability of the credit on Mobile User’s account is checked. Depending on the implementation multiple credit control and accounting messages may be exchanges during the on-going session.

3) Terminating phase- this phase terminates sessions between different entities of the infrastructure. Also in order to provide better charging and credit control transparency Charging Detail Records are requested by Mobile User for every session.

4.4.1.1 Phase 1: Authentication and Authorization

Authentication can be accomplished between Mobile User and ANP/TSP/VASP without a query to the 3P-AAA server. This may be accomplished through the use of the X.509 Certificate Infrastructure. In order to provide strong authentication features and mutual authentication of entities, a 3-Way Authentication should be employed. The benefit of the 3-Way Authentication is that it puts less stringent requirements for time synchronization between different devices employed. Since 3-Way Authentication only requires 3 signalling exchanges between two peers and our
infrastructure is based on the request/response model, the last message response carries authentication decision back to the party that initiated the authentication procedure.

Figure 17: Session outline
Even though authentication can take place without referral to the 3P-AAA server, when a request for resource usage is sent, the local ANP/TSP/VASP server will be queried whether the Mobile User has permission to access this resource. Depending on the charging implementation of the particular type of service, a credit control check will be performed in case if the online charging is used. Also since no assumptions should be made as to the geographical location of the 3P-AAA server and the level of the network congestion, Credit Control request should be sent by ANP/TSP/VASP towards the 3P-AAA server on the first round of the 3-Way Authentication procedure. This will allow to reduce the time delay and to have an authorization decision ready by the final round of the authentication procedure. Once authentication is accomplished, the decision of the authorization will be forwarded to
the Mobile User notifying of the results of the authentication and authorization procedures.

Figure 18 displays a Mobile User who wants to get an access to an Access Network managed by the ANP1 and then to access some services provided by the TSP1. In both cases authentication and authorization procedures are performed.

- A Mobile User wants to access services provided by ANP1. A 3P-AAA-MU-Initiation message is sent towards ANP1 gateway. The address of ANP may be received via Wireless Billboard Channel (WBC) [34] service, DHCP server or can be manually configured. During this stage ANP1 gains knowledge of the MU’s identity.

- A 3P-AAA-Start-Request is issued by ANP1 on the reception of the initiation message. ANP1 issues Session ID for this session and forwards start request to MU. This Session ID will be contained within every signalling message exchanged during this session. In order to complete authentication procedure, the MU and the ANP need to exchange their corresponding X.509 Certificates. The ANP attaches its Certificate to the request message. X.509
v3 Certificates allow inclusion of a number of private extensions to provide more flexible and optimized services.

- A 3P-AAA-Start-Answer is returned from Mobile User as an acknowledgement that it will continue participation in the session with the MU’s Certificate attached.
- Having received ANP’s Certificate, the MU can now complete the first step of the 3-Way Authentication procedure. The 3P-AAA-Auth-Request contains message that will include at minimum a timestamp, a nonce, an ID of ANP and a number of additional extension.
- A Credit-Control-Request message is sent towards the 3P-AAA server to verify that the MU has sufficient credit to access the ANP.
- Having MU’s Certificate at its disposal, the ANP1 can continue with the second step of the authentication procedure, extracting relevant information from the MU’s Certificate and sending a 3P-AAA-Auth-Answer towards MU containing a timestamp, nonce received previously from the MU as well as a nonce generated by the ANP1 itself, MU’s ID and a session key signed with MU’s public key.
- The 3P-AAA-Auth-Request completes the last step of the X.509 3-Way Authentication procedure. The intent of the third step is to address synchronization issue between devices. The information related to the authentication procedure includes return of the nonce previously generated by the ANP1 back to ANP1 for verification.
- Prior to completing the last step of the Authentication procedure, the ANP1 server waits for a Credit-Control-Answer message and makes authorization decision based on that message as well as on the identity of the user and the service requested.
- The MU receives the 3P-AAA-Auth-Answer message signalling the result of the authentication and authorization procedures.
- Once the ANP authentication and authorization is complete and both parties are satisfied with results, the MU repeats the above steps in order to complete TSP1 authentication. The message exchange between the MU and the TSP1 is similar.

Figure 19 describes interactions in case when the offline charging is performed by the system:

- A Mobile User wants to access services provided by the ANP1. 3P-AAA-MU-Initiation message is sent towards ANP1 gateway. The address of the ANP may be received via Wireless Billboard Channel (WBC) service, DHCP server or can be manually configured. During this stage, the ANP1 gains knowledge of the MU’s IPv6 address.
- A 3P-AAA-Start-Request is issued by the ANP1 on the reception of the initiation message. The ANP1 issues Session ID for this session and forwards start request to MU. This Session ID will be contained within every
signalling message exchanged during this session. In order to complete authentication procedure the MU and the ANP need to exchange their corresponding X.509 Certificates. The ANP attaches its Certificate to the request message. X.509 v3 Certificates allow inclusion of a number of private extensions to provide more flexible and optimized services.

Figure 19: Authentication and Authorization (Offline Charging)

- **3P-AAA-Start-Answer** is returned from the Mobile User as an acknowledgement that it will continue participation in the session with the MU’s Certificate attached.
- Having received ANP’s Certificate, the MU can now complete the first step of the 3-Way Authentication procedure. The **3P-AAA-Auth-Request** contains message that will include at minimum a timestamp, a nonce, an ID of ANP, optionally a session key signed with ANP’s public key and a number of additional extension.
Since the service requested uses the offline charging, no 3P-AAA solicitation takes place and the authorization decision made by the ANP1 is local, based on the authorization privileges and considerations of the network provider.

Having MU’s Certificate at its disposal, the ANP1 can continue with the second step of the authentication procedure, extracting relevant information from the MU’s Certificate and sending a 3P-AAA-Auth-Answer towards MU containing a timestamp, nonce received previously from the MU as well as a nonce generated by ANP itself, MU’s ID and session key signed with MU’s public key.

The 3P-AAA-Auth-Request completes the last step of the X.509 3-Way Authentication procedure. The intent of the third step is to address synchronization issue between devices. The information related to the authentication procedure includes return of the nonce previously generated by the ANP1 back to ANP1 for verification.

The MU receives the 3P-AAA-Auth-Answer message signalling the result of the authentication and authorization procedure.

Once ANP authentication and authorization is complete and both parties are satisfied with results, the MU repeats the above steps in order to complete the TSP1 authentication. The message exchange between the MU and TSP1 is similar.

### 4.4.1.2 Phase 2: Access Phase

The following scenario looks at the signalling that takes place when the Mobile User gets access to some service within ANP/TSP/VASP. Once the authentication and authorization process completes successfully, the Mobile User should be able to access the service requested. In case if the Mobile User is not aware of the charges applied for the requested service, the 3P-AAA-Price-Enquiry-Request/Answer messages may be exchanged between the Mobile User and the corresponding ANP/TSP/VASP.

Depending on the charging implementation of the ANP/TSP/VASP and type of the service accessed, multiple interrogations of the 3P-AAA server may be performed during the session. In case if access was authorized for multiple resources, Credit Control messages exchanged may belong to the same session but have different Sub-Session Ids.

Figure 20 shows the messages exchanged when the Mobile User is trying to access some services that implement online (real-time) charging. The following steps take place:
Prior to establishing association with ANP/TSP/VASP entities, the Mobile User may inquire about the charges applied for the services that the MU seeks. The 3P-AAA-Price-Enquiry-Request messages may be sent towards the corresponding ANP/TSP/VASP servers. Service ID as well as the IP addresses of ANP/TSP/VASP gateways may be received through the WBC service. The 3P-AAA-Price-Enquiry –Answer should contain full information regarding the charges applied.

Figure 20: Service Delivery (Online Charging)
• If after checking the price, the Mobile User is still interested in using the services offered by ANP/TSP/VASP, in order to gain access to the network a mutual authentication is performed between the MU and the ANP1 based on the X.509 Certificate Authentication. During this stage ANP1 will check availability of the credit on the MU’s account and will reserve certain amount of credit depending on the service in question.

• Having successfully accomplished authentication and authorization phase, the Mobile User gains access to the service, i.e. network coverage in this case. Since online charging offers a flexible charging and credit control framework, the 3P-AAA1 will maintain session and monitor use of the reserved credit. A number of intermediate updates will be exchanged between the 3P-AAA1 and the ANP1 servers.

• Once network coverage is available, the Mobile User may want to access certain teleservices. In order to do that, the mutual authentication takes place between the Mobile User and the corresponding TSP/VASP. During this phase the MU’s account will be checked and credit reserved for use of TSP/VASP’s service.

• If both, the ANP1 and the TSP1, authentication and authorization phases were successful, the Mobile User has gained access to the services. In typical scenario where session online charging is performed a number of intermediate Credit-Control-Request/Answer messages will be exchanged. These messages are usually triggered by some mid-service events such as updates about the amount of used units, requests for additional credit reservation etc.

• The Final Credit Control message exchanges takes place either when user has finished using services and notifies the corresponding ANP/TSP/VASP that he/she wishes to disconnect or when the reserved units were consumed and not replenished. Messages exchanged during this stage will be described in the next section.

Offline charging (Figure 21) does not implement credit monitor and control and only reports accounting data back to the 3P-AAA server. This type of charging infrastructure is typical of the subscriber services.

• The MU wants to access services offered by ANP/TSP/VASP. First, an inquiry is made about the prices and charges applicable. This information is delivered by means of 3P-AAA-Price-Enquery-Request/Answer messages.

• The Mobile User goes through authentication stage in order to gain access to the ANP1’s service. Since for this scenario offline charging is implemented, the 3P-AAA server consultation and credit reservation is not performed.
If the authentication and authorization were successful, the Mobile User can gain access to the access network. The ANP1 will start reporting accounting data to the 3P-AAA server.

If the Mobile User is wishing to access some teleservices, he/she has to go through authentication and authorization process once more with the corresponding TSP/VASP.

If authentication and authorization between the Mobile User and the TSP/VASP were successful, the Mobile User can start using a teleservice and the TSP/VASP will report accounting data to the 3P-AAA server.

Depending on the implementation of the offline charging a number of intermediate accounting messages may be periodically exchanged followed by the final STOP message indicating termination of the accounting stream (shown in the next section).

Figure 21: Service Delivery (Offline Charging)
4.4.1.3 Phase 3: Termination Phase

During the termination stage different entities have to be notified of the session teardown. In a typical scenario when a user gains access to resources, makes use of them and finishes session, a 3P-AAA-Termination-Request is sent towards the ANP/TSP/VASP entity. Reception of the Termination Request signals final credit control/accounting. After terminating current session the Mobile User sends request to the 3P-AAA for its Charging Detail Record. Enabling this feature would provide for better charging and billing transparency as the Mobile User would be able to compare the usage claimed by the ANP/TSP/VASP versus her/his own records.

Figures 22 and 23 show interactions that take place during the session termination stages for online and offline scenarios, respectively.

- The Mobile User has finished and wants to terminate session. The 3P-AAA-Termination-Request message is sent towards the TSP/VASP.
- The TSP/VASP now knows that the Mobile User will not use any more resources and thus the final Credit Control (for online charging) or Accounting (for offline charging) messages may be exchanged to finalize data about the use of resources.
- The TSP/VASP can now tear down its session with the 3P-AAA server by exchanging Session-Termination-Request/Answer messages.
- Once session is torn down between the TSP/VASP and the 3P-AAA, a 3P-AAA-Termination-Answer is sent to the Mobile User signalling that the session can be safely terminated.
- After the session has been terminated, the Mobile User wants to ensure that the correct charges and use of resources statistics have been applied. Mobile User sends a 3P-AAA-CDR-Request directly to the 3P-AAA through ‘b’ interface. This message includes Session ID of recently terminated session.
- The 3P-AAA satisfies MU’s query by embedding its CDR within a 3P-AAA-CDR-Answer.
- If the MU does not issue any further requests for teleservice use and wishes to terminate its session with ANP it goes through the same steps as described above, this time addressing the ANP entity.
Figure 22: Session Termination (Online Charging)
Scenario described above assumes that the Mobile User notifies the serving ANP/TSP/VASP prior to disconnecting. However, in some cases Mobile User may logoff or terminates session suddenly, without notification. In order to ensure connectivity the 3P-AAA-Ping-Request/Answer messages will be exchanged. This mechanism of insuring that the connection is alive is employed by the Diameter base protocol. As stated in the Authentication, Authorization and Accounting Transport Profile (RFC3539) [36], peer should not disconnect until timer expires at least twice. Thus when the timer has expired twice and not reset, the ANP/TSP/VASP will deduce that the connection has been abruptly terminated and will signal a session tear down as demonstrated in Figure 24.
The Mobile User device suddenly disconnects, for example, due to the device hardware failure. When this event occurs all other session participants are yet unaware of this failure.

At some point, depending on the timer settings, the MU and the ANP/TSP/VASP exchange keep-alive messages in the form of the 3P-AAA-Ping-Request/Answer messages. Once the TSP/VASP notices that a 3P-AAA-Request message has not been responded to and the ping request timer has been expired twice, the TSP/VASP will initiate session termination. It will do so by first exchanging the final Credit-Control or Accounting messages.

Once resource utilisation has been reported to the 3P-AAA server, Session-Termination-Request is sent to notify the 3P-AAA of the session tear down. On reception of the Session-Termination-Answer session is terminated.

Down the line the ANP will notice that the user has disconnected and go through the same set of steps as the TSP/VASP.

Once Mobile User will turn on the device, information about previously aborted sessions would allow user to issue a 3P-AAA-CDR-Request towards
the 3P-AAA server supplying Session IDS of the last ANP/TSP/VASP connections.

4.4.1.4 Phase 4: Re-Authentication and Re-Authorization

For variety of reasons, such as link failures or security related issues, Mobile user should be able to re-authenticate itself to the serving ANP/TSP/VASP and vice versa. Since X.509 Certificates have been previously exchanged, a 2-Way Authentication will be sufficient to re-authenticate entities to each other. In order to perform re-authorization, in cases when the online charging is used for the service in question, the 3P-AAA server will be consulted. Otherwise the ANP/TSP/VASP will make its own authorization decision. Figure 25 represents a case when the ANP wishes to re-authenticate and re-authorized. The same steps take place when the TSP/VASP wants to perform re-authentication and re-authorization.

Figure 25: ANP Re-Authentication and Re-Authorization (Online Charging)

Figure 26 describes an event where the ANP re-authorization has failed. Thus the MU/ANP session has to be terminated. Since Access Network is not available anymore, the current TSP/VASP session would have to be terminated as well. In case if the TSP/VASP re-authorization has failed, the TSP/VASP session termination will have no effect on the state of the ANP session.

- The ANP wants to perform re-authentication and re-authorization. Re-Authentication takes place through use of the X.509 2-Way Authentication procedure. Re-Authorization is a task performed by the ANP server in conjunction with a consultation as to the state of the MU’s account with the 3P-AAA server.
When either the ANP re-authentication or re-authorization has failed, the ANP/MU session has to be terminated. Due to the dependent nature of the TSP/VASP sessions on ANP’s transport, ANP’s session termination will force the TSP/VASP session to terminate as well.

ANP performing re-authentication and re-authorization will notify the Mobile User that it wishes to terminate session by sending 3P-AAA-Termination-Request specifying the reason for it within an AVP.

Next, the MU will notify the TSP/VASP and the TSP/VASP will go through the regular session termination procedure described in the previous section.

The ANP will perform its final Credit-Control message exchange, terminate session with the 3P-AAA server and then disconnect the MU session once it has received a 3P-AAA-Termination-Answer.

Once session is terminated, the user will issue a 3P-AAA-CDR-Request toward the 3P-AAA server.

### 4.4.1.5 Replenishing Account Credit

Often it might be the case that the Mobile User would run out of credit while accessing real-time charging resources of the ANP/TSP/VASP. When the Mobile User gets to the point of accessing his last credit units set aside, the Final-Unit-Indication AVP within the Credit-Control-Answer message should notify the user.
Once the Mobile User is aware that his/her credit is about to run out, the ANP/TSP/VASP would place restrictions on the access to the resource but the session will remain in the open state. Also it should be possible to replenish account as a single event through direct Mobile User to 3P-AAA-SP interface outside of any data access session. Mobile User simply sends a 3P-AAA-Credit-Request indicating the units that should be added to his/her account.

Four main scenarios may be distinguished here:

1) The ANP receives an update and the Mobile User buys more credit
2) The ANP receives an update and the Mobile User lets the Validity Timer to run out
3) The TSP/VASP receives an update and the Mobile User buys more credit
4) The TSP/VASP receives an update and the Mobile User lets the Validity Timer to run out

Since the decision taken by the Mobile User when ANP receives an update also triggers events at the TSP/VASP level, this scenario is reviewed in greater detail.

- In Figure 27 the MU is accessing ANP’s resource with the ANP periodically sending updates to the 3P-AAA to perform credit control monitoring. When the credit set aside is about to expire, the 3P-AAA will receive Final-Unit-Indication AVP.
- Reception of the Final-Unit-Indication AVP will trigger the ANP to send a 3P-AAA-Update-Request notifying the MU that the account has to be replenished.
- In the meantime the 3P-AAA server sets the Validity Timer and the ANP places restrictions on the use of its resources but not actually terminating the session.
- Since one of the possible outcomes of the signalling may be session termination, the MU informs the TSP/VASP that the final credit unit has been reached. Since ANP and TSP/VASP, depending on the service in question, set their account reservations separately, by the time the MU exhausts credit reserved for an ANP resource, credit reserved for a TSP/VASP resource might still be un-used.
- On the reception of a 3P-AAA-Update-Request from the Mobile User, TSP/VASP informs the 3P-AAA of the event and in turn receives the Validity Time from the 3P-AAA. Now the TSP/VASP places restriction on the use of its resources as well.
- Wishing to continue to participate in the session and to access ANP/TSP/VASP resources, the MU issues a 3P-AAA-Credit-Request to replenish account indicating the amount of monetary units. If transaction was
successful, the MU will be notified by the 3P-AAA server within corresponding 3P-AAA-Credit-Answer message.

• The ANP triggers authorization thus checking MU’s replenished account and reserving more credit. Once the ANP is happy with the results of the Credit-Control-Answer it will remove the restrictions imposed.
• The TSP/VASP will also perform authorization, receive Credit-Control-Answer and removed the restrictions. Since, while access was restricted, no session was terminated, the ANP/TSP/VASP sessions would retain their original Session IDs.
Figure 28 gives an example of an unsuccessful replenishment procedure. Just as in the previous scenario, the MU is accessing some online charging services. At some point the reserved credit is about to run out. And the ANP is notified of that.

In order to inform the MU that the credit replenishment is required a 3P-AAA-Update-Request messages is sent.

In the meantime the 3P-AAA server sets the Validity Time and notifies the ANP using a Credit-Control message. While account is not replenished, the ANP resources are restricted but the session is still active.
• The TSP/VASP service, having a different credit reservation instance, is still notified by means of the 3P-AAA-Update-Request of the possible ANP session termination. The reason for that is that the restriction placed by ANP has a direct effect on TSP/VASP session.

• TSP/VASP sends an update to the 3P-AAA server and receives the Validity Time set by the 3P-AAA. Now the TSP/VASP also puts restrictions on access to its services.

• In case if the Mobile User is unwilling to replenish credit by the time the ANP timer expires, ANP session termination procedure will take place.

• A 3P-AAA-TerminationRequest is sent out towards the Mobile User. Since TSP/VASP session cannot take place without ANP’s transport, the TSP/VASP session termination takes place first, followed by the ANP’s session tear down. Also since termination is triggered at ANP level and TSP/VASP has to follow suit or to perform vertical handover, it might be the case that when the MU/TSP/VASP session termination takes place some reserved units are still available and should be credited back to the Mobile User’s account by the 3P-AAA.

4.4.1.6 Failover Mechanism

Any infrastructure dealing with the accounting and collecting information related to charging should be able to handle connection failures and provide some sort of failover mechanism. One of the big advantages of the Diameter protocol in comparison to its predecessor RADIUS is that Diameter provides a failover mechanisms.

When the connection with the 3P-AAA server is lost any resilient network will have an alternative secondary server set up for storage of the session related data. In some cases that may not be possible when the routing of the messages is enforced to the specific fixed destination. Also it is stated by the Diameter Base protocol that the failover may produce a number of duplicate request messages and therefore care should be taken in detecting and removing these duplicates.

If the 3P-AAA server implementing Credit Control detects a failure during an ongoing session it terminates current session and returns the units reserved back to Mobile User’s account.

When the failure is detected by the ANP/TSP/VASP, i.e. the Credit Control client, two principal scenarios are possible. While the retry timer is running the ANP/TSP/VASP maintains session with the Mobile User and tries to reconnect with the 3P-AAA or to divert credit control and accounting data to an alternative server. Once the timer expires twice, depending on ANP/TSP/VASP implementation, it may
terminate session with the Mobile User or keep granting the service, locally storing the session related data and sending it to the server later when the connection is re-established. When this data is received by the 3P-AAA server, it will trigger ANP to send a 3P-AAA-Update-Request notifying the Mobile User that the data has been sent to the 3P-AAA server. Reception of the 3P-AAA-Update-Request will cause the Mobile User to send a 3P-AAA-CDR-Request to ensure that all the charges were applied properly.

Scenarios that may be considered, depending on the ANP/TSP/VASP implementation:

1) The ANP/3P-AAA interface connection has failed; TSP/VASP/3P-AAA is functional. ANP chooses to continue granting service, collecting and storing accounting data locally.
2) The ANP/3P-AAA interface connection has failed; TSP/VASP/3P-AAA is functional. ANP chooses to disconnect. This choice would affect the MU/TSP/VASP connection.
3) The TSP/VASP/3P-AAA interface connection has failed; ANP/3P-AAA is functional. TSP/VASP chooses to continue granting services.
4) The TSP/VASP/3P-AAA interface connection has failed; ANP/3P-AAA is functional. TSP/VASP chooses to disconnect.
5) Both ANP and TSP/VASP have lost connection to the 3P-AAA server.

Figure 29 displays signalling interactions when the ANP/3P-AAA interface connection fails and as a result sessions with the MU are terminated.

- During an on-going online charging session the ANP sends credit control update towards the 3P-AAA and receives no response. Also there is a mechanism embedded within the Diameter Base protocol that periodically checks whether connection is alive by means of the Device-Watchdog-Request/Answer messages. At some point the ANP will send new Device-Watchdog-Request and start timer waiting for response from the 3P-AAA. While timer is active session between the Mobile User and the ANP is active as well.
- The 3P-AAA server also periodically performs checks to ensure that the connection is still active. Having detected connection failure the 3P-AAA server disconnects and returns any unused reserved credit back to the MU’s account.
- Next the TSP/VASP session termination will follow the suit and complete its session. Since TSP/VASP still has connection with the 3P-AAA it would be able to complete the final Credit-Control in case if service implements the online charging or STOP accounting message to finalize accounting stream in case if the offline charging for this service is implemented.
Since there is no connection to the 3P-AAA server, ANP cannot perform final Credit-Control update back to the server. However, unused reserved units have already been credited back to MU’s account.

Once session has been terminated, the MU will send 3P-AAA-CDR-Request towards the 3P-AAA. Even if the ANP that was previously used for transport provision is unable to transport these messages to the 3P-AAA, there are
could be other ANPs within this area. If no alternative ANP is available, the MU will have to back off and try again later.

Figure 30: Failover (ANP continues granting services)

- In comparison to the previous scenario, Figure 30 shows signalling for an ANP, which will continue providing services to the Mobile User in case of the failover. Since ANP does not terminate, the Mobile User is completely agnostic as to the state of the ANP/3P-AAA connection. The MU will continue using whatever ANP/TSP/VASP services it had previously accessed.
- Once the Mobile User has finished utilizing resources, TSP/VASP session termination will take place as usual.
- Once the TSP/VASP session is over, if the MU does not want to access any other teleservices, ANP session termination will be signalled by means of a 3P-AAA-Termination-Request. Since there is still no connection to the 3P-AAA server and all of the Credit-Control information is collected by the ANP server, no final Credit-Control update can reach the 3P-AAA server.
- A 3P-AAA-Termination-Answer is issued by the ANP allowing the MU to terminate session. However, some AVP has to indicate to the MU
application’s state machine not to send a *3P-AAA-CDR-Request/Answer* message toward the 3P-AAA server. The reason being is that even if an alternative ANP would be able to transport these messages to the 3P-AAA server, the information that the server currently holds is incomplete until it receives an update from the ANP.

- Once connection has been re-established, the ANP will forward all the charging or accounting information that it collected while connection was down. Once Credit-Control-Answer is received from the 3P-AAA server, the ANP will inform the Mobile User within a *3P-AAA-Update* that now it can send *3P-AAA-CDR-Request*. Once *3P-AAA-Update-Answer* has been received, the ANP can disconnect.

- Having received an update from the ANP, the MU has been signalled that it can issue a *3P-AAA-CDR-Request* towards the 3P-AAA server.

An observation can be made that in case when the connection fails between ANP/TSP/VASP and the 3P-AAA and ANP/TSP/VASP is implemented to provision services and accounting data storage, the charges generated may be greater than the actual credit available on the user’s account. When connection is re-established and charging data is forwarded to the server, the 3P-AAA would have to debit these charges from the user’s account. It might be a sensible idea to allow users to overdraw their accounts up to certain monetary amount.

**4.4.2 HAC Related Scenarios**

**4.4.2.1 Introduction**

One of the key issues that should be addressed within the context of heterogeneous networks is the handover techniques. Handover techniques can be viewed and classified according to a number of different parameters: soft and hard, vertical and horizontal, network controlled and mobile-assisted.

Hard handover is the type of handover that was typically employed by the analog telecommunication technologies and provides less flexibility and larger switching delays than the currently employed handoff techniques. It can be summarized that the hard handover technique is of the type *break-before-make* where current session will be disconnected and channel released and only then a new channel connection will be initiated. This technique is much easier to implement, however, it inhibits the problem of delays. Since nowadays channels do not only carry voice data where some delays and loss of data may be tolerated but also IP packets, this technique is not suitable due to its flexibility limitations. On the other hand soft handover finds alternative channel and initiates connection set up and only once alternative channel is available and ready for use, releases the old connection.
In older GSM networks the decision for handover was taken by the mobile operator. However with the growing importance of the QoS requirements, the need for a mobile-assisted handover emerged. With mobile assisted handover (MAHO) mobile equipment measurements have influence on the handover decision.

Another classification of handover can be seen from the perspective of the vertical or horizontal handover. Horizontal handover usually means that the mobile user changes its point of attachment without change of the access technology. Different horizontal handover mechanisms are implemented by different cellular and wireless technologies. Some scenarios may involve not only the change of the attachment point but also of the administrative domain. When Layer 3 (IP) handoff takes place, new IP address has to be allocated in the new domain. In general this distinction between what is considered to be user’s Home domain and the Visited domain gives rise to differentiation in services available to the user and not only in the technical sense, but also differentiation in charges applied. UCWW proposes allocation of a single globally significant identifier (IPv6 address) [37] that will be associated with a user. This identifier will be used to gain access to teleservices regardless of the geographical location and to apply charges incurred.

Vertical handover is a relatively new concept that allows a single device to use multiple wireless interfaces to access network services. A number of currently available mobile devices are able to handle not only cellular networks but a number of other wireless access technologies such as WLAN, WiMAX and Bluetooth. Thus, within heterogeneous networks where a number of access technologies may be available to the mobile user the ability to switch between different access technologies is of paramount importance. In other words, teleservices available to the mobile user should be decoupled from the technology used to access them. Vertical handover can be divided into three principle phases: network discovery, handover decision and handover implementation. We will assume that the network discovery is outside the scope of this document.

Based on the above a number of conclusions can be made and applied to the HAC (Hot Access network Change) handover. The handover framework should be flexible implementing soft mobile-assisted handover and should be able to handle horizontal and vertical handoffs. As mention in [38] handover decision may be initiated by the Mobile User or the TSP/VASP entities when QoS fall beyond certain level guaranteed by the TSP/VASP or the ANP. Also it should be mentioned that for the purposes of this thesis what is important is the signalling application layer data generated during the handover procedure.

4.4.2.2 Vertical Handover Issues

At the moment one of the most robust architectures integrating cellular, WLAN and WiMAX access provisions is developed by the 3GPP. In general 3GPP architecture
closely follows the principles of loose coupling and high cohesion, where a number of elements perform very specific tasks. The issue of mobility and handover are closely woven. Previously mobility issues have been addressed at the IP level and a number of mobility solutions have been proposed: Mobile IPv6 [39], Hierarchical Mobile IP (HMIP) [40] etc. The downside of these schemes is the existence of the additional entities, such as Home Agent, and significant handover delays and overhead. Also due to the development of Internet a need for a new Transport protocol was emerging. SCTP protocol was introduced combining some of the properties of TCP and UDP with additional enhanced features suitable for modern day computing: multi-homing and multi-streaming. Combined with Dynamic Address Reconfiguration [41] extension SCTP can be used for seamless handover without additional functional entities. Using SCTP multi-homing feature and the ability to dynamically add/delete IP addresses to multiple device interfaces the mobile devices can move between different access networks maintaining its association with a remote server. Research has been carried out proposing different solutions [42-44] to vertical handover problem with slight alterations indicating the possibility of seamless handover with minimal service disruption.

4.4.2.3 User Triggered HAC

Scenarios described in this section form an important part of the overall user experience. One of the limitations of the current wireless/cellular networks is that once the user is connected to an ANP and accesses some services he/she does not have the ability to switch access technology on-the-fly and continue with an ongoing session. In the context of UCWW when the Mobile User is within an area that has several access technologies, he/she should be able to switch an on-going session from cellular to wireless IP access if that change produces certain benefit from the financial and QoS level perspective. One of the possibilities is to include access service pricing information as an additional factor of the QoS metrics, i.e. QoS level variable can be composed of a number of physical parameters such as a bit rate, jitter, packet drop rate probability and a variable associated with the price. Depending on the type of the subscription with a 3P-AAA-SP this parameter may have different weight and thus have an influence on the choice of the ANP. Also care should be taken in the calculation of the QoS threshold as it may lead to a ping-pong effect where handoff signalling takes place back and forth thus producing unwanted overhead. User triggered HAC scenario can be envisioned when the MU, being connected to the ANP and accessing services provided by the TSP, may will to perform vertical handover switching to a different service provider. Typically, if the QoS level drops suddenly when accessing the service it should be the responsibility of the TSP/VASP to initiate HAC. Thus the most probable scenario for this case is when the Mobile User wishes to procure access to cheaper access coverage.
In Figure 31 the Mobile User has established an online charging session with ANP1 and establishes another session with TSP1. During this session the Mobile User is signalled that the QoS level has changed below certain threshold established or has received an update from the WBC notifying that another access network with higher QoS is available. The Mobile User chooses to perform the handover. The Mobile User initiates new connection to the ANP2 and goes through the initial process of Authentication and Authorization at the same time maintaining its current sessions with the ANP1 and the TSP1.

Once Authentication has been successful the Mobile User can avail of services provided by the ANP2. At the same time while connection to the ANP2 takes place, the TSP1 should be notified by means of the Update message that handover is about to take place, supplying identifier of the candidate access network.

When connection to ANP2 is established the Mobile User is currently connected to two access networks. Using the mSCTP (Mobile SCTP) features the Mobile User currently has multi-homed association with TSP1. Now stream of data can be reconfigured to take primary route path of the new ANP2 while closing the old ANP1 stream connection.
• Since transport layer data has been successfully moved to the stream associated with the new ANP2, the Mobile User initiates Session Termination with the ‘old’ ANP1.
• Closing of ANP1 session should have no effect on the session between the Mobile User and the TSP1, which continue to exchange the Credit Control messages.

4.4.2.4 TSP/VASP Triggered HAC

The TSP/VASP Triggered HAC describes the situation when the TSP/VASP server is not satisfied with the QoS level provided by the current access networks. When the Mobile User initiates session with TSP/VASP and accesses services, a certain level of QoS is guaranteed. If the access network is congested it would produce drop in the data rate and might not be satisfactory in term of required parameters for a teleservice. Thus in order to fulfil its obligations in terms of the QoS before its customer, the TSP/VASP would initiate the HAC procedure. In this case the extra charges that might be incurred when switching to an alternative access provider will be paid by the TSP/VASP.

• In Figure 32 the Mobile User has established session with ANP1 and TSP1 to access some teleservices. At some point the QoS of the teleservice falls beyond threshold level due to the access network problems. Since TSP1 is committed to provision of teleservice at certain QoS level it triggers the HAC procedure.
• Once decision is taken to perform HAC, the TSP1 notifies the Mobile User of its decision through an update messages signalling an alternative access network that the Mobile User should initiate connection to.
• Having indication of the handover procedure, the Mobile User will initiate another connection with the ANP2 by going through normal stages of a set up procedure that involves Authentication and Authorization steps. As indicated in [38] the Mobile User should include identifier of the ‘old’ ANP1 in its request messages.
• Once the Mobile User has received a new IP address from the ANP2 its Transport Layer can perform stream handover using mSCTP by dynamically adding the new IP address to the association. Once the new primary route has been set to include the newly assigned ANP2 address the ‘old’ ANP1 address can be deleted thus completing the soft handover of the data stream.
• In the upper layer the ANP1 Session Termination procedure takes place.
• Access to the teleservice provided by the TSP1 continues with consequent exchanges of the Credit Control information. It should be noted that the Credit Control exchanges related to the charges applied by the ANP2 are paid.
by the Mobile User but at the rate less than or equal to that of the ANP1. In case if extra charges were incurred during the HAC procedure, the TSP1, being the originator, will pay the extra-costs.

4.4.3 Novel 3P-AAA Scenarios

Flexibility of the 3P-AAA gives rise to the additional scenarios that might take place in UCWW:

- Switching teleservice provider during an on-going session
- Multiple ANP sessions when using teleservice(s) to enable asymmetric service delivery
- TSP chaining involving two or more TSPs and/or VASPS in provision of a teleservice to the user

4.4.3.1 TSP change

When discussing TSP-triggered HAC, first, classification of the teleservices should be established. Two principle types of services may be distinguished here:
1. Services that require disconnection of the old and initiation of the new session. Most of the teleservices would fall into that category. One of the issues here is that these services are stateful and the information about their state is of the local significance. Services such as web browsing (using cookies or tokens), location and presence services, games and data download would fall into this category.

2. Services where session is established with another Mobile User and may be handed over during an on-going session (Figure 33); this criterion would apply to voice or video transmission streams shared between participating nodes and applications such as VoIP or teleconferencing.

Figure 33: User triggered HAC with TSP change

Figure 34 demonstrates an example where the Mobile User is accessing some real-time charging teleservice:

- During an on-going session, the QoS level guaranteed by the TSP1 falls beyond allowed threshold value.
- While maintaining session with the original TSP, the MU is initiating a new connection with a service similar to the currently used but provided by the TSP2. The diagram above only covers signalling related to the 3P-AAA infrastructure. Any additional teleservice specific signalling is outside the scope of this description.
- If Authentication and Authorization steps are successfully completed by the MU, he/she can now access TSP2 service.
- Since new connection has been established, the session connection to the old TSP1 can now be terminated by invoking the session termination procedure.
- Once the TSP1 has been disconnected, sessions continue with the corresponding ANP1 and TSP2.
4.4.3.2 Multiple serving ANPs

Availability of several network access technologies in the given geographical region is a common modern day reality. Typically within metropolitan area a number of WAN, MAN and LAN access technologies would overlap. Since the whole idea of the 3P-AAA is to enable easy access, there should be provision to enjoy extended utilization of the available access resources. In case if the Mobile User is wishing to access services from TSP(s) in the region where multiple access technologies overlap, it should be possible to simultaneously have active sessions through different ANPs.

Figure 35 above demonstrates an example where MU1 is accessing services offered by the TSP1. Depending on the bandwidth requirements of each service accessed, media stream may be routed through two distinct ANPs with different access technologies. For example, delay sensitive real-time service traffic may be accommodated by the faster ANP. Decision to perform this kind of service access should also take into account the user subscription profile with 3P-AAA.
In technical terms the SCTP’s multi-homing feature may be used to provide stream delivery through different paths. At the moment, even though SCTP provides multi-homing capability where multiple paths may exist between source and destination, this feature is only employed for failover and retransmission. This limitation is due to the fact that these mechanisms have been inherited from TCP. However, since more and more emerging devices accommodate multiple network interfaces it is very probable that these issues will be addressed and resolved in the near future. Some SCTP schemes and multi-homing optimizations have been suggested in [45, 46].

![Diagram of Access to teleservice(s) through different ANPs](image)

Figure 35: Access to teleservice(s) through different ANPs

When the Mobile User connects to some ANP, this ANP guarantees certain level of service that can be translated into some physical parameters such as bandwidth, throughput, queuing delays etc. At the same time accessing services provided by TSP, services also have some requirements in terms of physical and data link parameters. In case if a total requirement for services is greater than that provisioned by the currently serving ANP, two possibilities may be considered here:

- To look for an alternative ANP that would satisfy TSP’s requirements
- To establish session with another ANP and to distribute service access between newly connected ANPs

Some mechanism may be provided by the network to quantify physical aspects and to provide selection algorithm that would take into account not only physical parameters but also the customer’s profile preferences.

As an example consider scenario where the Mobile User is located in the area with N access network providers and is wishing to access K services offered by TSP(1). Assuming that QoS is some non-negative real number used to quantify parameters, following simple algorithm might be used:

1. Evaluate total resource requirements:

   \[ QoS_{\text{Total}} = \sum_{k=0}^{n} QoS \]
2. Compare resources available at the current ANP with resources required to satisfy all the requests
3. If amount of resources provided by the current ANP is less than the amount required, look for a minimal combination of N ANPs that would satisfy service requirements
4. Once found, distribute media flow between these ANPs

As can be noticed from Figure 36, in signalling terms, the message flow is similar to that of the user triggered HAC procedure for change of the ANP. The principle difference here is that instead of the session termination with ANP1, service delivery will continue through both ANPs.

4.4.3.3 Service Delivery Chaining

Flexibility presented by the 3P-AAA framework will influence expansion of the Value Added Service (VAS) supply since it would produce a more favourable environment for development and deployment of these services. Value Added Services may be defined as non-core services that provide some additional functionality to the basic services and may function as stand-alone services. VASPs provide greater service market diversification and specialization by targeting specific
group of customers. Often VASPs might require some additional resources for provision of their services.

Currently most of the VAS are implemented and deployed by the mobile operators. As a result, in order to gain access to some VAS and applications, a mobile user first needs to create a service level agreement with a mobile operator.

In [47] authors present good market classification and categorizations of m-commerce VAS offered by the Taiwanese mobile operators. This paper reviewed 40 service types with over 200 Value Added Service items offered by the mobile operators and classified them according to a number of criteria. The three major factors in the categorization are:

- The extent of dependence on the location
- The extent to which application is time critical
- Whether it is controlled by the mobile user or by the Service Provider

Based on the permutation of the above factors 8 possible arrangements may be produced:

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Information that is both timely and related to the immediate environment</td>
</tr>
<tr>
<td>II</td>
<td>Similar to I but controlled by the product or service provider</td>
</tr>
<tr>
<td>III</td>
<td>On-demand provision of information regarding physical environment of the recipient</td>
</tr>
<tr>
<td>IV</td>
<td>Similar to I but not time critical</td>
</tr>
<tr>
<td>V</td>
<td>Acquisition of time-critical information that is tied to a remote transaction</td>
</tr>
<tr>
<td>VI</td>
<td>Similar to V but initiative rests with information provider</td>
</tr>
<tr>
<td>VII</td>
<td>Receiver initiated information acquisition stored in a repository or database</td>
</tr>
<tr>
<td>VIII</td>
<td>Modification or configuration software for remote mobile users</td>
</tr>
</tbody>
</table>

In the above research most of the services fall within categories VI (182), IV (38) and I (13). However, the cases studied by this research are related to VAS offered by the mobile operator and not 3rd party VASPs. Also the 3GPP specifications provide examples of the types of services supported: SMS, MMS, Account Management, Terminal Status, Terminal Location, Multimedia Conferencing, Group List Management, Presence Services, Geocoding, Application Driven QoS, and Content Management etc.
One of the key ideas of the 3P-AAA framework is to stimulate teleservice diversity through decoupling of access and teleservice provisions. It is very likely that some of the value-added services already offered by the mobile operator would remain under the management of the access operator even in the UCWW, but it is going to be the new emerging teleservices and value-added services that would be mostly interested in the deployment within the 3P-AAA infrastructure.

Currently network operators are similar to the middle man between the 3rd party VASP and the end-user. Since charging and billing infrastructure has quiet strict implementation requirements, 3rd party VASPs utilize ANPs infrastructure for these purposes. There are two business models in operation regarding the 3rd party VAS: VASP provider sells an application to an operator or VASP hosts an application and utilizes ANPs charging infrastructure, thus the end user is billed by ANP on behalf of VASP.

As can be seen from the Figure 37 [48] a Service Delivery Platform (SDP) acts as a broker between VAS and Service Enablers. Once 3rd party VASPs registered with the SDP, its application will have access to Service Capabilities provided by the Service Enablers. Some 3rd party VAS may require more than one service capability from the network; these applications are called Composite Applications. As outlined in the 3GPP technical specification document regarding Open Service Access (OSA) [49], the principle tasks of the SDP are authentication, application registration, discovery and charging. Communication between these entities is handled by the OSA/Parlay Interface. Trying to put this framework in the perspective of the 3P-AAA, the following observation can be made:
• Authentication procedure can be performed through exchange of X.509 Certificates
• Services provided by the application as well as services offered by the Service Enablers may be registered and made discoverable through other UCWW entities (ADA activity [2])
• Charging will be performed through the c interface connecting VASP and the corresponding 3P-AAA-SP

Thus SDP may be removed and replaced by the direct communication between 3rd party VASP requiring additional resources and the TSP/ANP offering them through an a interface.

Figure 38: Service Delivery Chaining Example

Figure 38 demonstrates an example where the MU1 is wishing to access services of the VASP1. This service may have been advertised through the WBC. Once session is established with the VASP1, the need for additional resources might arise for which TSP1 will be consulted. From the perspective of the TSP1, the VASP1 that is currently utilizes its resources is no different than the typical mobile client.

• In Figure 39 the MU1 has established a session connection with VASP1. During this session the accounting and credit control data is exchanged between the 3P-AAA1 and VASP1 server. When the connection was established the VASP1 guaranteed provision of certain service with the corresponding level of QoS.
• If VASP1 requires some additional resources in order to successfully provide services, these resources can be purchased from the ANP or the TSP. At the moment, this kind of a framework exists within 3GPP IMS. To successfully fulfil its part of the service delivery, the VASP1 contacts the TSP1. Also in this case, mobile user is completely agnostic as to the interactions that happen between the VASP1 and the TSP1.
• Since the VASP1 and the TSP1 a priori do not share any security association, the Authentication and Authorization has to be first performed.
• If the Authentication and Authorization was successful, the VASP1 can now access resources of the TSP1. The TSP1 will maintain accounting and credit
control stream with the corresponding 3P-AAA1 to monitor resources consumed by the VASP1.

- As can be seen from the diagram, the three credit control streams exist in this scenario: between the ANP1 and the 3P-AAA1 on behalf of the resources consumed by the MU1, between the VASP1 and the 3P-AAA1 on behalf of the resources consumed by the MU1 and between the TSP1 and the 3P-AAA1 on behalf of the resources consumed by the VASP1.

Figure 39: Service Delivery Chaining

Figure 40 displays details of the session termination procedure when the service chaining is involved. Session termination procedure is similar to that of the normal session; the principle difference is that the additional signalling takes place to terminate session between the VASP1 and the TSP1.
Figure 40: Chained Service Session Termination

4.5 3P-AAA and IMS integration

Services described by the UCWW framework are user-demand driven. In other words both SBM and CBM should be able to co-exist and occupy their corresponding niche in the market. It should be up to the users to evaluate and decide what services are better suited for their needs. Integration of 3GPP and 3P-AAA would allow mobile users to avail of services provided by both infrastructures. After making subscription with the 3P-AAA Service Provider and obtaining personal IPv6 address embedded within CIM (Consumer Identity Module) [37], the MU will be
able to gain access to the 3P-AAA services as well as to that of the user’s original Home Network.

Since the IMS has capability for provision of teleservices through the deployment of Application Servers and inclusion of VASP through the OSA infrastructure, it may be seen as an integrated access and teleservice provider. Deployment of the 3P-AAA framework will have an impact on the way teleservices are being offered not only from the point of view of the users but also of the TSPs. If previously TSPs and VASPs had to have a contractual relationship with the access network providers, now they could be considered as separate standalone entities. Thus, seeing the benefits offered by the 3P-AAA, any TSP/VASP that previously had a contractual relationship with the ANP would be able to break away and entrust its AAA management to a 3P-AAA service provider.

Consider a scenario where the MU is wishing to access some value-added service. Currently, the way to do this would be through the Home ANP. When the 3P-AAA is integrated with the existing IMS, as shown in the Figure 41 [50], MU will be able to establish session directly with TSP/VASP through the interface ‘a’.

![Figure 41: 3P-AAA and IMS integration](image)

4.6 Conclusion

This chapter has covered a lot of material describing different aspects of the 3P-AAA framework. The material presented here integrates certain technical aspects discussed in the previous chapters related to signalling and security. First, a higher level overview of the 3P-AAA framework was given. Since UCWW utilizes certain
concept-specific terms in the description of the framework, these terms are properly explained, e.g., ANP, TSP etc. The 3P-AAA signalling is at the core of the framework and most of the chapter is dedicated to the description of the transactions that take place by means of the envisioned interfaces. Each interface is designed to interconnect specific entities of the framework. In order to realize requirements needed for the implementation of the outlined interfaces, a number of scenarios and used cases have been reviewed. Basic signalling scenarios look at the interactions that take place when a single user is wishing to access single set of resources from the access- or tele-service provider. These scenarios include cases when both, online and offline, charging models are applied. In the cases involving handover, the new 3P-AAA specific HAC technique is outlined. In general, design of the 3P-AAA framework allows for the emergence of new signalling cases that would not be possible in the SBM world. These possibilities will have an impact on not only the way the mobile users access services, but also to the way these services are offered to them. Important thing to realize, is that the UCWW environment does not suggest complete removal of the legacy technology but rather a peaceful co-existence, where it would be up to the customers to decide which technology should become prevalent. The importance of this chapter is that it helped to identify messaging requirements that should be provisioned by the 3P-AAA signalling protocol. With the help of the case scenarios, these messages and their corresponding attributes will be formally defined in the next chapter.
CHAPTER 5

3P-AAA SIGNALLING

5.1 Introduction

Previous chapters have covered some technical background, where a number of signalling protocols have been mentioned. At the same time, chapter 4 looked at the different forms of interactions that might take place in the 3P-AAA environment. Based on the research outlined in the precedent chapters, this chapter sets out to formally outline the principle signalling messages and attributes required to fulfil the 3P-AAA signalling functionality. The first issue that would be addressed is what signalling protocol should be used as a foundation of the 3P-AAA signalling protocol. Good choice of the protocol is very important as it will have serious impact on the future performance of the framework implementations. Having chosen the right protocol and taking into account its format, new messages will be define to provide the minimal functionality of the 3P-AAA framework. In order to outline these messages in an orderly manner, first a set of messages for each interface of the 3P-AAA framework will be outlined, followed by the section summarizing all the new principle attributes related to these messages.

5.2 3P-AAA Protocol Stack

Previous sections have covered three signalling protocols that could be considered for implementation of the 3P-AAA: SIP [Section 2.8], PANA [Section 2.6] and Diameter [Section 3.3]. Table III below compares given protocols according to criteria listed on the left-hand side.

Table III: Comparing signalling protocols

<table>
<thead>
<tr>
<th></th>
<th>SIP</th>
<th>PANA</th>
<th>Diameter Base</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transport</strong></td>
<td>SCTP, TCP, UDP</td>
<td>UDP</td>
<td>TCP, SCTP</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>HTTP Digest AKA (in 3GPP), TLS X.509 certificate.</td>
<td>EAP negotiated (X.509 certificates proposed)</td>
<td>Application defined</td>
</tr>
<tr>
<td><strong>Scalability</strong></td>
<td>Scalable through SIP agents</td>
<td>Not scalable</td>
<td>Scalable through Diameter agents</td>
</tr>
</tbody>
</table>
Two principle approaches may be considered for the 3P-AAA implementation. The first approach can use the extended 3P-AAA Diameter for end-to-end signalling. 3P-AAA Diameter may use some of the PANA features to support authentication since both protocols have similar structure, where information is conveyed by means of AVP messages [51]. This approach would provide the AAA and Credit Control functionality for the three interfaces. In this configuration, the access router would operate as a Diameter Proxy, which is capable of modifying the message content and, therefore, provide value-added services, enforce rules and policy on different messages, or perform administrative tasks for a specific realm. This thesis adopts this approach and lists 3P-AAA messages and their corresponding AVP codes in the next section. Thus the protocol stack shown in Figure 42 will be adopted by the 3P-AAA signalling application [50]. Using the modular approach for the implementation of the protocol stack would allow for a more convenient maintenance or the addition of the new features.

The second approach can use SIP signalling between the MU and the access router, and Diameter on the inside of the network. Disadvantage of this approach is that the message translation would be required to extract information from SIP messages in order to form Diameter messages. However, some elements of this approach can be seen in the IMS, where Call/Session Control Function performs similar tasks. On the positive side, the use of SIP would provide a wider range of additional functionality as this protocol supports media stream negotiations and presence services.

The main reason why the 3P-AAA signalling protocol needs to borrow from other signalling protocols or to be based on them, is because this way the useful features of the underlying protocols can be re-used. This is especially important from the implementation point of view. Such features as resilience and error handling mechanism are especially important which makes the build-up of the new 3P-AAA features safer and more reliable when built on top of the protocols that have been widely tested and deployed in the industrial environment.

<table>
<thead>
<tr>
<th>Presence and Location Management</th>
<th>Able to provide presence and mobility information</th>
<th>Not available</th>
<th>Not available</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wide Spread Use</strong></td>
<td>Wide use in multimedia environment. Used by 3GPP’s IMS.</td>
<td>Not very common</td>
<td>Envisioned to replace RADIUS (the currently used AAA protocol). Used by 3GPP’s IMS.</td>
</tr>
</tbody>
</table>
5.3 Messages and AVPs

Table IV below outlines the primary messages used in the 3P-AAA infrastructure per each interface. As can be seen from the table, messaging borrows heavily on the ideas outlined in PANA and Diameter Base and Credit Control Applications [51]. Most of the AVPs used in signalling have been outlined in the corresponding Internet Engineering Task Force (IETF) Request For Comments (RFC) documents. The newly devised AVPs and their details are listed in the following section..

<table>
<thead>
<tr>
<th>Messages over Interface ‘a’ (MU ↔ ANP/TSP/VASP)</th>
<th>Messages over Interface ‘b’ (MU ↔ 3P-AAA)</th>
<th>Messages over Interface ‘c’ (ANP/TSP/VASP ↔ 3P-AAA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3P-AAA-MU-Initiation(3P-AAA User Application)</td>
<td>3P-AAA-Get-Credit-Request/Answer(3P-AAA User Application)</td>
<td>Credit-Control-Request/Answer(Diameter Credit-Control)</td>
</tr>
<tr>
<td>3P-AAA-Start-Request/Answer(3P-AAA User Application)</td>
<td>3P-AAA-Check-Balance-Request/Answer(3P-AAA User Application)</td>
<td>Re-Auth-Request/Answer(Diameter Base)</td>
</tr>
<tr>
<td>3P-AAA-Auth-Request/Answer(3P-AAA User Application)</td>
<td>3P-AAA-CDR-Request/Answer(3P-AAA User Application)</td>
<td>Session-Termination-Request/Answer(Diameter Base)</td>
</tr>
<tr>
<td>3P-AAA-Ping-Request/Answer(3P-AAA)</td>
<td></td>
<td>Abort-Session-Request/Answer(Diameter Base)</td>
</tr>
</tbody>
</table>
### 5.3.1 Messages over Interface ‘a’

#### 3P-AAA-MU-Initiation

MU uses this message to initiate session connection with an ANP or a TSP [17, 51]. It is assumed that the IP address of these entities is supplied through WBC service. This message is used to supply ANP or TSP with the MU’s identity. At this point Session-Id AVP is set to 0.

\[
3P-AAA-MU-Initiation ::= < 3P-AAA-Header: N >
\quad \{\text{Origin-Host}\} \text{ Section 6.3 of [27]}
\quad \{\text{Origin-Realm}\} \text{ Section 6.4 of [27]}
\quad \{\text{Destination-Realm}\} \text{ Section 6.6 of [27]}
\quad *[\text{AVP}]
\]

#### 3P-AAA-Start-Request

Once an initiation message has been received, ANP or TSP responds with a 3P-AAA-Start-Request message. Since X.509 Certificate will be required to mutually authenticate session participants, ANP/TSP sends its certificate in the start request message along with the session identifier allocated to the current session. In order to ensure message integrity during the session, ANP/TSP negotiates the integrity algorithm.

\[
3P-AAA-Start-Request ::= < 3P-AAA-Header: N,R >
\quad <\text{Session-Id}\> \text{ Section 8.8 of [27]}
\quad \{\text{Origin-Host}\}
\]
As response to the start request, corresponding node will reply to the ANP/TSP with a message that will contain its X.509 Certificate that will be used later during the Authentication procedure. Using integrity algorithm suggested by ANP/TSP, the MU will apply algorithm to the message load.

3P-AAA-Start-Answer

3P-AAA-Auth-Request

Authentication request message addresses the issue of mutual node authentication in the 3P-AAA environment. This procedure is based on the X.509 Certificates that were previously exchanged. Request messages will also include some session parameters, such as session timers and routing permissions, set by ANP/TSP and may also contain credit control and accounting AVPs.

3P-AAA-Auth-Answer
This message is used to carry information and AVPs related to the 3 way authentication procedure as well as the result of the authentication procedure.

3P-AAA-Auth-Answer ::= < 3P-AAA-Header: N >
    <Session-Id>
    {Result-Code}
    {Origin-Host}
    {Origin-Realm}
    {Destination-Realm}
    {Nonce}
    {Event-Timestamp}
    {Digital-Envelope}
    {Session-Timeout}
    {Service-Context-Id}
    *(AUTH)
    *[AVP]

3P-AAA-Ping-Request

Ping messages are used to check session’s aliveness and for failover mechanism purposes [17, 51]. Requests may be initiated by either MU or ANP/TSP. It is ANP/TSP that sets ping timer. Event-Timestamp AVP may be included here to provide some statistical data for trip delays etc.

3P-AAA-Ping-Request ::= < 3P-AAA-Header: N,R >
    {Origin-Host}
    {Origin-Realm}
    {Destination-Realm}
    {Ping-Timer} 3P-AAA specific
    [Event-Timestamp]
    *[AVP]

3P-AAA-Ping-Answer

This message is sent as a response message to a ping request.

3P-AAA-Ping-Answer ::= < 3P-AAA-Header: N >
    {Result-Code}
    {Origin-Host}
    {Origin-Realm}
    {Destination-Realm}
    {Event-Timestamp}
    *[AVP]

3P-AAA-Termination-Request
Message is used to indicate session termination procedure. This message can be originated by either MU or ANP/TSP. The reason for session termination is given in the Termination-Cause AVP.

3P-AAA-Termination-Request ::= < 3P-AAA-Header: N,R >
  <Session-Id>
  {Origin-Host}
  {Origin-Realm}
  {Destination-Host}
  {Destination-Realm}
  {Termination-Cause}Section 8.15 of [27]
  *[AVP]

3P-AAA-Termination-Answer

Message is send as a response to the termination request.

3P-AAA-Termination-Answer ::= < 3P-AAA-Header: N >
  {Result-Code}
  {Origin-Host}
  {Origin-Realm}
  {Destination-Realm}
  [Failed-AVP] Section 7.5 of [27]
  *[AVP]

3P-AAA-Update-Request

Update message is used as an informative message in the 3P-AAA Diameter application. It is used in scenarios related to credit replenishment, failover, handover etc. Since ANP session may have an impact on TSP session, for example, in cases when ANP has to be switched, update message is used to coordinate these actions.

3P-AAA-Update-Request ::= < 3P-AAA-Header: N,R >
  {Origin-Host}
  {Origin-Realm}
  {Destination-Realm}
  [Hot-Access-Change] 3P-AAA specific
  [Replenishment-Indicator] 3P-AAA specific
  [CDR-Notification] 3P-AAA specific
  *[AVP]

3P-AAA-Update-Answer

This message is issued as response to the update request.

3P-AAA-Update-Answer ::= < 3P-AAA-Header: N >
3P-AAA-Price-Enquiry-Request

This message is used to check price of access or teleservices [29, 51]. Must support AVPs defined by the Credit Control Application.

3P-AAA-Price-Enquiry-Request ::= < 3P-AAA-Header: N,R >
   {Origin-Host}
   {Origin-Realm}
   {Destination-Realm}
   {Service-Context-Id}
   *[AVP]

3P-AAA-Price-Enquiry-Answer

This message is issued in response to the price enquiry request.

3P-AAA-Price-Enquiry-Answer ::= < 3P-AAA-Header: N >
   {Result-Code}
   {Origin-Host}
   {Origin-Realm}
   {Destination-Realm}
   {Service-Context-Id}
   {Cost-Information} Section 8.7 of [29]
   {CC-Money} Section 8.22 of [29]
   *[AVP]

3P-AAA-ReAuth-Request

Re-authentication request may be issued by either ANP/TSP server or the MU. Re-authentication may be performed by the MU before Authorization-Lifetime expires or issued by ANP/TSP server during account replenishment procedure. Since both corresponding entities possess their counterpart’s X.509 Certificates, 2 Way authentication is performed.

3P-AAA-ReAuth-Request ::= < 3P-AAA-Header: N,R >
   <Session-Id>
   {Origin-Host}
3P-AAA-ReAuth-Answer

Re-authentication answer sent as a response to the re-authentication request message.

3P-AAA-ReAuth-Answer ::= < 3P-AAA-Header: N >
   <Session-Id>
   {Result-Code}
   {Origin-Host}
   {Origin-Realm}
   {Destination-Realm}
   {Nonce}
   {Event-Timestamp}
   {Session-Timeout}
   [Error-Message]
   *(AUTH)
   *[AVP]

5.3.2 Messages over Interface ‘b’

3P-AAA-Get-Credit-Request

This message is sent directly to the 3P-AAA-SP and is seen as a request to allocate MU’s credit towards use of some ANP or TSP service. Variable units may be used for credit allocation such as time or monetary value.

3P-AAA-Get-Credit-Request ::= < 3P-AAA-Header: N,R >
   <Session-Id>
   {Origin-Host}
   {Origin-Realm}
   {Destination-Realm}
   {Service-Context-Id}
   [CC-Money]
   [CC-Service-Specific-Units] Section 8.26 of [29]
   [Cost-Unit] Section 8.12 of [29]
   [Currency-Code] Section 8.11 of [29]
   [Value-Digit] Section 8.10 of [29]
   *(AUTH)
   *[AVP]
3P-AAA-Get-Credit-Answer

Reply message to the credit request message.

3P-AAA-Get-Credit-Request ::= < 3P-AAA-Header: N,R >

3P-AAA-Check-Balance-Request

This message allows the MU to check his/her account balance.

3P-AAA-Check-Balance-Request ::= < 3P-AAA-Header: N,R >

3P-AAA-Check-Balance-Answer

A message sent as a response to the balance request. This message contains Result-Code AVP typical for Diameter requests as well as Check-Balance-Request defined by the Credit Control Application.
3P-AAA-CDR-Request

This message provides accounting and credit control transparency within the 3P-AAA framework. It is by means of this message that the customer is able to keep record of his/her resource usage. Every session initiated by the MU should have a corresponding Charging Detail Record.

```
3P-AAA-CDR-Request ::= < 3P-AAA-Header: N,R >
  <Session-Id>
  {Origin-Host}
  {Origin-Realm}
  {Destination-Realm}
  {Service-Context-Id}
  *(AUTH)
  *[AVP]
```

3P-AAA-CDR-Answer

CDR answer is send as a response to the CDR request for this session. This message contains an Universal-3p3a-Charging-Detail-Record AVP as described in [38]

```
3P-AAA-CDR-Answer ::= < 3P-AAA-Header: N,R >
  <Session-Id>
  {Result-Code}
  {Origin-Host}
  {Origin-Realm}
  {Destination-Realm}
  {Service-Context-Id}
  {Universal-3p3a-Charging-Detail-Record}
  [Error-AVP]
  *(AUTH)
  *[AVP]
```

5.3.3 Messages over Interface ‘c’

Messages identified in this section address communication between the Diameter Server and the ANP/TSP. These messages use Diameter Base [27] and Credit Control [29] defined messages with some additional 3P-AAA AVPs.

Credit-Control-Request

Message used to provide online accounting and credit control capabilities within the 3P-AAA infrastructure. Message is inherited from the Credit Control Application
and is exchanged between Credit-Control Client (ANP/TSP Server) and Credit-Control Server (3P-AAA Server).

Credit-Control-Request ::= < Diameter Header: 272,R >
  <Session-Id>
  {Origin-Host}
  {Origin-Realm}
  {Destination-Realm}
  {Auth-Application-Id}
  {Service-Context-Id}
  {CC-Request-Type} Section 12.5 of [29]
  {CC-Request-Number} Section 8.2 of [29]
  [ CC-Sub-Session-Id ] Section 8.5 of [29]
  {Origin-State-Id} Section 8.2 of [29]
  {Event-Timestamp}
  [Service-Identifier] Section 8.28 of [29]
  [Termination-Cause]
  [Requested-Service-Unit] Section 8.18 of [29]
  *[ Used-Service-Unit ] Section 8.19 of [29]
  [ Multiple-Services-Indicator ] Section 8.40 of [29]
  *[ Multiple-Services-Credit-Control ] Section 8.16 of [29]
  [HAC-Initiator] 3P-AAA specific
  *[AVP]

Credit-Control-Answer

Answer messages sent as a result of the Credit-Control-Request used in the variety of scenarios involving real-time accounting and credit control.

Credit-Control-Answer ::= < Diameter Header: 272 >
  <Session-Id>
  {Result-Code}
  {Origin-Host}
  {Origin-Realm}
  {Auth-Application-Id}
  {CC-Request-Type}
  {CC-Request-Number}
  [CC-Session-Failover] Section 12.6 of [29]
  [CC-Sub-Session-Id]
  [Acct-Multi-Session-Id]
  [Event-Timestamp]
  [Granted-Service-Unit]
  *[Multiple-Services-Credit-Control]
  [Cost-Information]
  [Final-Unit-Indication] Section 8.34 of [29]
  [Check-Balance-Result]
  [Credit-Control-Failure-Handling] Section 8.14 of [29]
  [Direct-Debiting-Failure-Handling] Section 8.15 of [29]
  [Validity-Time]
  *[Redirect-Host]
  *[Redirect-Host-Usage]
  *[Proxy-Info]
  *[Route-Record]
Re-Auth-Request

This re-authentication request, in contrast to re-authentication described within interface a, is originated by the 3P-AAA server with intention of signalling to the ANP/TSP that the MU re-authentication should take place. This could be done for security reason when server session timer has expired.

Re-Auth-Request ::= < Diameter Header: 258, R >
< Session-Id >
{Origin-Host}
{Origin-Realm}
{Destination-Realm}
{Destination-Host}
{Auth-Application-Id}
{Re-Auth-Request-Type}
{Origin-State-Id}
* [Proxy-Info]
* [Route-Record]
* [AVP]

Re-Auth-Answer

This message is sent as a response to the re-auth request by the corresponding party.

Re-Auth-Answer ::= < Diameter Header: 258 >
{Origin-Host}
{Origin-Realm}
{Destination-Host}
{Destination-Realm}
{Failed-AVP}
* [AVP]

Session-Termination-Request

Just like the termination request specified by the 3P-AAA Application, Diameter Session-Termination-Request is used to signal session termination to the corresponding node.

Session-Termination-Request ::= < Diameter Header: 275, R >
< Session-Id >
{Origin-Host}
{Origin-Realm}
{Destination-Realm}
{Auth-Application-Id}
{Termination-Cause}
Session-Termination-Answer

Diameter session termination answer is sent as a response to the termination request.

Session-Termination-Answer ::= < Diameter Header: 275 >
  < Session-Id >
  {Result-Code}
  {Origin-Host}
  {Origin-Realm}
  {Error-Message}
  [Error-Reporting-Host]
  * [Failed-AVP]
  {Origin-State-Id}
  * [Redirect-Host]
  {Redirect-Host-Usage}
  * [AVP]

Abort-Session-Request

Abort request may be sent by the Diameter server towards resources provider as a result of network failure.

Abort-Session-Request ::= < Diameter Header: 274, R >
  < Session-Id >
  {Origin-Host}
  {Origin-Realm}
  {Destination-Realm}
  {Destination-Host}
  {Auth-Application-Id}
  {User-Name}
  {Origin-State-Id}
  * [Proxy-Info]
  * [Route-Record]
  * [AVP]

Abort-Session-Answer

Message sent as a response to the abort request.

Abort-Session-Answer ::= < Diameter Header: 274 >
  < Session-Id >
  {Result-Code}
  {Origin-Host}
  {Origin-Realm}
  [User-Name]
Accounting-Request

Accounting messages would be typically used by the services and applications that do not require online charging. This message facilitates an exchange of the accounting data for resources and services used.

Accounting-Request ::= < Diameter Header: 271, R >
   < Session-Id >
   {Origin-Host}
   {Origin-Realm}
   {Destination-Realm}
   {Accounting-Record-Type}
   {Accounting-Record-Number}
   [Acct-Application-Id]
   [Vendor-Specific-Application-Id]
   [Acct-Session-Id]
   [Acct-Multi-Session-Id]
   [Acct-Interim-Interval]
   [Accounting-Realtime-Required]
   [Origin-State-Id]
   [Event-Timestamp]
* [Proxy-Info]
* [Route-Record]
* [AVP]

Accounting-Answer

Diameter base accounting answer message is used to carry responses to the accounting request messages.

<ACA> ::= < Diameter Header: 271 >
   < Session-Id >
   {Result-Code}
   {Origin-Host}
   {Origin-Realm}
   {Accounting-Record-Type}
   {Accounting-Record-Number}
   [Acct-Application-Id]
   [Vendor-Specific-Application-Id]
   [User-Name]
   [Accounting-Sub-Session-Id]
   [Acct-Session-Id]
   [Acct-Multi-Session-Id]
Disconnect-Peer-Request

This message is used by the Diameter protocol to notify peer as to the reasons of the transport disconnection. As stated within the RFC 3588, the corresponding peer usually does not know the reason for disconnection and might assume it to be the result of the transport level failure with following periodic attempts to re-establish connection. Disconnect-Cause AVP, carried by the disconnect request, ensures that in some cases no action should be taken to re-establish connection.

Disconnect-Peer-Request ::= < Diameter Header: 282, R >
{Origin-Host}
{Origin-Realm}
{Disconnect-Cause}

Disconnect-Peer-Answer

Sent as a response to the disconnect request.

Disconnect-Peer-Answer ::= < Diameter Header: 282 >
{Result-Code}
{Origin-Host}
{Origin-Realm}
{Error-Message}
* [Failed-AVP]

Device-Watchdog-Request

Device Watchdog is an application level mechanism that is used to proactively detect transport failures. The exact mechanism is described in [36].

Device-Watchdog-Request ::= < Diameter Header: 280, R >
{Origin-Host}
{Origin-Realm}
{Origin-State-Id}
Device-Watchdog-Answer

This message is sent as a response to the device watchdog request.

Device-Watchdog-Answer ::= < Diameter Header: 280 >
{Result-Code}
{Origin-Host}
{Origin-Realm}
{Error-Message}
* [Failed-AVP]
[Original-State-Id]

Capabilities-Exchange-Request

These messages are used by Diameter to discover peer’s identity and capabilities. In case if corresponding peer does not share any common Diameter applications or security mechanisms, request originator will be notified of that through Result-Code AVP. It is also stated by the RFC 3588 that these messages must not be proxied, relayed or redirected. Since SCTP may be used as a transport protocol, this request should contain a Host-IP-Address AVP for each IP address that may be locally used when transmitting Diameter messages.

Capability-Exchange-Request ::= < Diameter Header: 257, R >
{Origin-Host}
{Origin-Realm}
1* { Host-IP-Address } section 5.3.5 of [27]
{Vendor-Id}
{Product-Name}
[Origin-State-Id]
* [Supported-Vendor-Id]
* [Auth-Application-Id]
* [Inband-Security-Id]
* [Acct-Application-Id]
* [Vendor-Specific-Application-Id]
[Firmware-Revision]
* [AVP]

Capabilities-Exchange-Answer

Messages sent a response to the capability exchange requests.

Capability-Exchange-Answer ::= < Diameter Header: 257 >
{Result-Code}
{Origin-Host}
{Origin-Realm}
1* {Host-IP-Address}
{Vendor-Id}
{Product-Name}
[Origin-State-Id]
[Error-Message]
5.4 3P-AAA AVPs

Apart from the AVPs provided by the Diameter Base protocol and the Credit Control Application, some additional AVPs have been defined to support the 3P-AAA functionality. These AVPs have been drawn based on the requirements deduced from the signalling scenarios [53] as well as functionality of the PANA protocol [34].

Certificate

This AVP is of type OctetString and is used to carry X.509 Certificates [51]. This AVP is used in the authentication procedure and will accompany 3P-AAA authentication requests messages in order to provide certificate exchange between the corresponding parties.

Integrity-Algorithm

The motivation for this AVP is taken from PANA protocol where it is used to negotiate integrity algorithm between the party requesting resources and the party allocating them. Unlike PANA that states this AVP to be of type Unsigned32, in 3P-AAA this AVP is of type Enumerated as this type is easier to implement in software and the number of integrity algorithms used hardly requires the full range provided by a 32 bit space.

HMAC-SHA1-160 0
HMAC-MD5-128 1

AUTH

AUTH AVP is borrowed from PANA where it used to ensure message integrity [17, 51]. This AVP is of type OctetString and contains message authentication code calculated from the result of the concatenation operation between the session key and the signalling message load.
Nonce

This AVP is of type OctetString and is used to carry a pseudo-randomly generated number. Nonce is employed during the authentication procedure in order to enforce cryptographic reply protection.

Digital-Envelop

AVP of type OctetString used to carry symmetric session key generated by the ANP/TSP and encoded with MU’s public key [51].

Ping-Timer

AVP of type Unsigned32 used to set timing interval used by the 3P-AAA ping messages to check the aliveness of the connection.

Hot-Access-Change

Hot-Access-Change AVP is employed to provide additional information between signalling nodes during HAC handover. It is of type Grouped and has the following structure:

Hot-Access-Change ::= < AVP Header: N >
  [HAC-Initiator]
  [Multiple-ANP-Provision]
  *[Old-Service-Provider]
  *[New-Service-Provider]

HAC-Initiator

An auxiliary type DiameterIdentity HAC AVP used to indicate the party that initiate the handover procedure. It is important for charging related information as the party that initiated HAC would be responsible for possible access charges.

Multiple-ANP-Provision

To provide grater flexibility and higher QoS, in some cases, depending on the MU’s subscription profile, it might be possible to employ multiple ANPs at the same time to ensure higher quality and rate of access. This AVP of type Enumerated is used to indicate to the ANP/TSP whether this type of provision is enabled.

MULTIPLE-ANP-PROVISION_ALLOWED 0
Old-Service-Provider

This AVP of type DiameterIdentity is used to signal the identity of the service provider, ANP or TSP, which is being switched.

New-Service-Provider

This AVP of type DiameterIdentity is used to signal the identity of the new service provider, ANP or TSP, towards which new session is being initiated by the 3P-AAA client.

Replenishment-Indicator

This AVP is of type UTF8String and contains value of the Service-Context-Id. It is used by the update message to indicate that further credit should be allocated to this particular service.

CDR-Notification

AVP of type Grouped employed by the update message in the scenario when due to disconnection with the 3P-AAA server, MU was not able to receive CDR. In this case, the service provider should notify the MU that connection was re-established and CDR should be requested.

CDR-Notification ::= < AVP Header: N >
{Session-Id}
{Service-Context-Id}

Universal-3p3a-Charging-Detail-Record

This AVP of type UTF8String contains charging detail record for each session. Charging Detail Records are used to enforce accounting and credit control transparency.

Termination-Cause

This Enumerated type AVP is part of the Diameter Base protocol and is used to convey the reason for session termination. Since some additional scenarios have
been outlined that are not provisioned by the original protocol, additional clauses should be added to the message.

3P-AAA_NO_TRANSPORT       9
3P-AAA_HAC                  10

5.5 Conclusion

Chapter 5 completes the 3P-AAA background research and design stage of the project. Previous chapters have provided information related to the technical details of the available signalling protocols and security mechanisms, the 3P-AAA framework layout and interface description culminating in the description of the 3P-AAA protocol, its protocol stack and the corresponding protocol messages.

In order to avoid definition of a completely new signalling protocol, which would require a significant research effort, this thesis chose to consider other application level signalling protocols that could be used as a base for the design of the 3P-AAA signalling. After thorough review of the candidate protocols, it was decided that the Diameter Base protocol would form basis of the 3P-AAA signalling also borrowing functionality of the PANA’s authentication. These two protocols can be combined together due to the similarity of its messaging formats. Use of Diameter would also allow implementation of the online and the offline charging using the Diameter Credit Control and Accounting. Additionally, in order to satisfy requirements for the novel interactions scenarios outlined in chapter 4, new messages and attribute-value pairs were defined. These messages were defined for each interface of the 3P-AAA framework.
CHAPTER 6

IMPLEMENTATION ISSUES

Careful architectural design is of paramount importance from the project management point of view as it allows to minimize implementation time and helps to eliminate certain conceptual errors. This thesis primarily addressed 3P-AAA design issues through careful examination of the framework architecture and signalling protocols. This section looks at the possible implementation methods that could be adopted for the creation of 3P-AAA infrastructure. The following protocol stack implementations will be discussed:

- OpenDiameter open source project [54]
- OpenBlox Diameter Base stack by TraffixSystems [55]
- J Diameter open source project from the Java.net community [56]
- Cpana open source project [57]

Additionally some licenced versions of the Diameter protocol stack will be mentioned: IntelliNet’s Accelero [58] and Marben’s Diameter [59]. Also some issues related to the possible 3P-AAA framework simulation will be outlined, where the principle tool is the Network Simulator 2 and 3 (NS2/3) [60, 61]. Based on the material discussed in this chapter recommendations will be made concerning implementation of the 3P-AAA framework.

6.1 Protocol Stacks

Software implementation of the Diameter Base protocol is needed to provide even basic implementation of the 3P-AAA signalling capabilities. Since Diameter is widely used in the IMS infrastructure, the biggest testing ground for this protocol has been organization of the IMS/NGN Plugfests. These events have been organized to bring together leading IMS and NGN software vendors, systems integrators, and service providers delivering cable, wireless, wireline and enterprise solution in order to see in what state the industry is currently in regarding IMS rollout and to ensure interoperability between different vendors. Up to date, eight Plugfest events have taken place where each event has been centred on specific set of issues. Based on the Plugfest results and findings, Forum’s Technical Working Groups publish white papers outlining IMS/NGN best practices and guidelines. A number of commercial stack implementations are available [62], IntelliNet’s Accelero and Marben’s
Diameter stack being examples. However, the protocol stack implementations offered by these companies do not provide access to the source code and only offer binary files. The problems with that is that even though new attributes and messages can be defined, the state machine cannot be modified and thus the interactions outlined in chapter 4 cannot be integrated. Another down side of the commercial software is its licence price.

6.1.1 OpenDiameter

OpenDiameter was the first open source implementations of the Diameter Base protocol. This stack has been developed in 2004, shortly after emergence of the protocol itself. It is based on a number of C++ libraries that are currently supported by Linux and Windows platforms. EAP and PANA protocols are also part of the OpenDiameter project. EAP stack supports a number of methods, such as EAP-MD5, EAP-TLS etc.

Core OpenDiameter libraries of the latest release are listed below:

- ibdiamparser: Diameter message parser library (with XML dictionary support), with capable of user-defined AVP type parsers
- lib Diameter: Diameter core engine library with base accounting support.
- lib Diametereap: Diameter EAP Application library
- lib Diameternasreq: Diameter NASREQ Application library
- libeap: EAP library
- lib Diametermip4: Diameter MIPv4 library
- EAP-Archie: A key-derivative EAP authentication method implementation
- EAP-TLS: A key-derivative EAP authentication method implementation (for Linux/FreeBSD only)

The OpenDiameter C++ API is a simple session based API with each type of Diameter session being represented by a C++ class. User applications derived from these session classes to implement their own specific AAA functionality. All events, message processing and message transmission functionality are provided by these classes. Generally, the session classes are categorized into either client or server. The client classes provided AAA client capabilities and server classes provide AAA server functions. These two types of classes are further sub-divided into either authentication/authorization classes and accounting classes.

The information stated above is listed in the OpenDiameter documentation. Even though OpenDiameter is widely used for research in academic community, it is very hard to find any coherent and truly in-depth information on its installation and use. Project’s web site [54] contains OpenDiameter project documentation, however, it is
poorly maintained and rarely updated. One of the problems is that Open Diameter itself depends on the number of other open-source software packages. The main prerequisites stated in the installation notes are:

1. GNU g++ used to compile the C++ libraries
2. Xerces C++ XML parser version 2.1.0 and higher that is used for parsing Diameter messages
3. ACE Library 5.5.0 Adaptive Communication Environment (ACE) is a freely available, open-source object-oriented (OO) framework that implements many core patterns for concurrent communication software.
4. Boost Library free peer-reviewed portable C++ source libraries
5. OpenSSL Library that implements the Secure Sockets Layer and Transport Layer Security

Some versions of the prerequisite software are conflicting with each other. It is stated that OpenDiameter can run on Linux as well as Windows 2000/XP, at the same time documentation warns against Windows installation claiming it to be unstable. Overall, installation of the software is very problematic not to mention development which requires very high level of programming expertise.

### 6.1.2 OpenBlox

OpenBlox Diameter Stack is offered by the TraffixSystems which is one of the companies that actively participates in the IMS/NGN Plugfest events. Unlike OpenDiameter, which is only available in C++ implementation, OpenBlox is available for C++ and Java platforms. Apart from implementation of the Diameter Base, the company also provides support for 55 interfaces standardized by the bodies like 3GPP, ETSI (European Telecommunication Standard Institute) and WiMax [55]. OpenBlox software along with interface implementation is available freely with an option of getting additional interfaces and software support with purchase of the licence. The fact that OpenBlox is software that has been tested in the industrial environment makes it more reliable and better maintained than the OpenDiameter. However, the problem with OpenBlox is that the services offered by the open software licence do not allow access to some parts of the program implementation and do not provide documentation outside of the basic interface set. Licenced version of the software, which includes additional interfaces, support and training, is well outside the financial reach of our academic project.

### 6.1.3 JDiameter

Another Diameter Base protocol implementation that was available in the open source development community is JDiameter that was offered as a Java implementation of the stack and whose libraries were available for download. The
site that hosted the project (www.Java.net), hosts a number of open source software projects implemented in Java. However, it seems that the project has been removed from the hosting website.

### 6.1.4 Cpana

Cpana is an open source software that implements PANA protocol in C programming language. The project is registered on the sourceforge.net from the August of 2010 [57]. As outlined in the README document attached to the project installation, Cpana contains the following code:

- cpana - PANA library
- ceap - EAP library
- clpe - library containing common miscellaneous functions for cpana and ceap.
- apps - contains example applications including cpaa (PAA) and cpac (PaC)

Looking at the documentation supplied by the project, it becomes evident that this implementation might not be very suitable for adoption due to the following reasons:

- this implementation only partially adheres to the underlying PANA and EAP standards
- the software documentation is very limited
- implemented programming language is very platform depended with the Cpana software written specifically for Unix adherent Linux and BSD platforms

### 6.2 Simulation Issues

Network simulation is a common technique that is used to test some behaviour of the real network virtually. Even though simulation can only be considered as an approximation to the real world environment, it is considered to be inexpensive and fast in the provision of useful quantitative metric regarding the abilities of the network. In the case of the 3P-AAA some parameters of interest would be the ones related to the signalling latency, scalability and responsiveness of the infrastructure. The most common tool used in the academic research is Network Simulator (NS) 2 [60] and the newer version NS 3 [61]. NS2/3 is open source software that provides a virtual simulation environment. It uses C++/Python written libraries to simulate some common protocol stacks for different levels of OSI stack. It also uses Object Tcl (OTcl) scripting to set up the simulation environment. The problem of NS2/3 is that it does not have Graphic User Interface (GUI) and requires certain level of expertise and understanding of scripting languages. A 3P-AAA simulation would require use of protocols such as mSCTP and 3P-AAA Diameter that are not available
in either version of the NS and thus have to be written from scratch. In general, developing this thesis we tend to have an abstract look at the lower levels of the OSI protocol stack. Simulation may help to evaluate how interactions and different scenarios involving different access technologies might influence the overall performance of the system.

### 6.3 Conclusion

Currently available protocol stacks are not well suited for the project implementation. One of the drawbacks of the OpenDiameter and Cpana is that both of these software packages are written in C/C++, languages that heavily depend on the underlying OS platforms. The source code produced is constrained to run on only limited set of the operation system environments typically Unix based, which seriously hinders portability. The solution to that problem would be to implement the 3P-AAA protocol in Java, which allows software to run on any device with a compatible Java Virtual Machine. Most of the modern handheld devices like mobile phones, smart phones, reading pads and laptops support JVM environment.

Since 3P-AAA introduces new features and scenarios that are not possible for most Diameter implementations, adaption of the new protocol outlined in chapter 5 would require changes to the protocol’s state machine in order to accommodate interaction scenarios described in chapter 4. Currently, none of the available off-the-shelf protocol stacks are suitable for this task. The reason being that the available software was developed to adhere to the common IETF or 3GPP standards that do not envision interactions outlined in the 3P-AAA framework. Probably, some of the libraries used by the open source software could be used as reference models, but in general in order to create the environment outlined by the 3P-AAA a totally new 3P-AAA-tailored software would have to be written from scratch.

Based on the description of the issues above, a statement can be issued that the implementation of the 3P-AAA signalling protocol would require good technical knowledge and experience in C++/Java programming as creation of the new robust software is a non-trivial matter.
CHAPTER 7

CONCLUSIONS AND FUTURE WORK

The main goal of this thesis was to set out the reason and the challenge of creating a new 3P-AAA infrastructure, and to demonstrate and discuss different aspects of the envisioned 3P-AAA infrastructure. That includes not only the details of the framework, like signalling protocols and participating entities, but overall motivation and reasons for the emergence.

As outlined in the introduction chapter, it is important to realize that the proposition made by the development of the 3P-AAA goes well beyond technological innovation. It gives a new perspective at the service offering in general. All the business models currently adopted in the telecommunication industry are built on the foundation of the subscription environment. Even though new business models introduce some form of innovation, their flexibility is inherently constrained by the structural limitations. 3P-AAA aims at removing these barriers through adoption of the Consumer-centric Business Model. Instead of the multiple subscriptions with numerous service offering entities, CBM requires only single entity to provide Service Level Agreement subscription- that of the 3P-AAA Service Provider. 3P-AAA-SPs will specialize in offering their services to a number of clients that would encompass ANPs, TSPs and, of course, Mobile Users.

This novel UCWW environment created by the combination of the CBM and 3P-AAA adoption will introduce a number of new scenarios and benefits that are not currently available to the typical end client. In this environment every mobile client would be able to enjoy full spectrum of services offered by the telecommunication industry. This includes control over the choice of the access provider services as well as numerous value added services whose offering will not depend on the underlying infrastructure of the access providers. This also invokes a number of benefits for the smaller and middle sized service providers. In general development of the charging and billing infrastructure is a complicated and money-demanding process. Decoupling of the charging and billing services from the underlying service provision would provoke a more active participation in the market of smaller service offering entities. This in turn would create a more competitive and thus more customer-beneficial environment centred on the end user demand.

Having outlined the principle goal of the 3P-AAA environment the question arises as to how these changes and environment can be accommodated. Chapter 2 performs an overview of the available technologies and frameworks that could be used as points of reference for the 3P-AAA development. Design of the 3P-AAA should include strong security features as well as robust and flexible modes of operation. 3P-AAA
uses a number of security related technologies such as IPsec, TLS and X.509 Certificates. The latter is used primarily for the user authentication in the wireless environment.

Communication between participating entities is of paramount importance for success of the project. Here the principle role is played by the appropriate choice of the signalling protocol as well as careful review of the salient features. A number of signalling protocols exist in the telecommunication industry; the most popular ones are RADIUS, SIP and Diameter. PANA is another protocol that has much to offer, however it is still not adopted by the industry and requires a more careful research and scrutiny from the academic community. Signalling employed by the 3P-AAA evaluates features of these protocols. Some additional features outlined by 3P-AAA are a novel vertical handover technique - Hot Access network Change (HAC). HAC enables Mobile User to make handover decisions based on the QoS levels of the access or teleservice in question. This may include cases of handover even when MU is not moving and is simply unsatisfied with the current service provision. In order to facilitate handover process at the lower levels of the OSI stack, it is considered that the transport profile of the SCTP with an extension that allows dynamic IP interface assignment should aid the handover process. Another feature that worth mentioning is that 3P-AAA signalling will provide direct communication between MU and serving 3P-AAA-SP. That signifies that services related to the account access will be accomplished directly through this interface and would include features like credit check, account top up etc. As a result of technical review of frameworks and signalling protocols, available and salient features are integrated into case scenarios. Later, based on these scenarios technical specification for 3P-AAA signalling is drawn with description of the messages and corresponding AVPs.

Of course, in real terms, every emerging technology should have provisions for integration and backward compatibility with legacy frameworks. This thesis looks at the possible co-existence between 3P-AAA framework and another 3G technology that is currently gaining momentum in the telecommunication industry- IP Multimedia Subsystems. IMS definition is a work of the 3GPP consortium and its main achievement is the decoupling of the access, control and service planes. IMS and 3P-AAA frameworks could possibly coexist in the telecommunication environment making it up to the user and other participating entities to decide what technology will be prevalent.

Diameter protocol with some adaptation is the principle protocol envisioned for 3P-AAA signalling. The chapter covering Diameter Base protocol has plenty of technical details but one of the most useful features of Diameter is its extensibility. Diameter Base framework is adopted by a number of other protocols as can be seen from the list of the available Diameter based applications. Maintenance and revision procedures always require significant effort in the IT industry. It is especially important for 3P-AAA signalling framework since a number of design features and
scenarios might have to be revised, altered or added during transition between design and implementation stages of the project.

The following section contains description of the future work for the project:

- Implementation of the 3P-AAA signalling- as discussed in the implementation issue section of the thesis, implementing 3P-AAA signalling possesses some serious challenges. Since protocol defines behaviour not outlined in the Diameter Base protocol and thus requires review of the state machine, 3P-AAA signalling implementation cannot use Diameter Base stack implementations currently available. Unless new software will emerge that allows redefinition of the state machine, it might be the case that the protocol will have to be implemented from scratch based on the requirements.

- Alternative SIP/Diameter Implementation- SIP is widely used for front-end signalling within IMS. It also provides a number of extended session control features well-suited for multimedia sessions. It might be beneficial to investigate the possibility of the front-end signalling involving SIP and back-end signalling involving Diameter. The disadvantages of this approach would be additional need for translation of received SIP messages into corresponding Diameter format. However, experience in that field can be borrowed from the IMS implementations. Also, this approach might be more appropriate for integration of IMS and 3P-AAA environments, since it would require minimal changes in the IMS signalling.

- Framework Simulation- with the creation of the 3P-AAA signalling application, simulation would have to be performed in order to provide some feel as to the functional environment of the framework. Simulation will also enable collection of some quantitative data. A choice of the appropriate simulation tool would have to be made. Common tools include NS2/3 and OPNET [63]. However, since 3P-AAA does not use standardized upper level protocols (Diameter extended 3P-AAA protocol and mSCTP), simulation would require additional technical expertise for the development of the additional libraries in order to simulate operational environment.

- Test Bed development- Simulation produces only approximated results of the real world operating environment. Even though simulation may provide better and cheaper scalability, for this project simulation would require extensive development effort. Thus a better approach might be the test bed development. Test bed might provide a useful inside in the operations of the overall framework and help to collect some useful data. Since it is hard to make predictions about physical performance parameters a priori, process of the overall interactions between different levels of the OSI stack should be monitored. These interactions may have a profound influence on the physical channel parameters such as signal latency when tested in the normal operating scenarios versus HAC involved operating scenarios.
Another issue that should be addressed, especially considering the importance of the charging data produced, is testing different security features and profiles. This may include strength of the X.509 Certificates along with additional IPsec and TLS features and how these additional features affect round-trip delay time.

- Design Re-evaluation- based on the results of the protocol implementation and test bed simulations overall re-evaluation of the design should be performed. This re-evaluation should address three prominent issues:
  - Possible changes to the 3P-AAA signalling protocol might include features built into the protocol itself. For example, use of the asymmetric cryptographic methods might be too costly or latent in the wireless environment. Some other cryptographic methods or combination of methods might be considered.
  - Overall evaluation of the protocol stack composition might signal some problems with the current design of the protocol stack, i.e. the combination of different layers of the OSI stack. For example, in order to accommodate vertical handover for HAC related scenarios SCTP was adopted due to its multi-homing features. In case if this transport profile shows poor performance, some other possibilities might be considered, i.e. UDP/TCP protocols in the Transport layer and MIPv6 [64] or HMIP [40] in the IP layer.
  - Optimization- in order to improve overall performance and to minimize signalling overhead, some optimizations to the original design should be considered. One possible optimization in order to minimize constant communication with the back-end server could be collection of the accounting/charging data at the local service providing entities that will later be sent over to the 3P-AAA-SP. Another possible optimization is temporary storage of the X.509 Certificates in order to minimize signalling for service providers that are often accessed by the same Mobile User.

- In case if implementation produces good results and after careful re-evaluation of the original design, the next logical step would be standardization of the 3P-AAA interfaces through formal submission of the Request For Commence (RFC) document to the Internet Engineering Task Force (IETF) standardization body.

**Research outcomes published to date**

- Dmitry Tairov, Ivan Ganchev, Máirtín O'Droma et al. (University of Limerick, Ireland). Ubiquitous Consumer Wireless World- Protocols Foundations and Standardization. URL: [http://www.globeforum.com/dublin](http://www.globeforum.com/dublin). This poster was presented at the Globe Forum Dublin, November 17, 2010
The poster outlined basic infrastructural layout of the 3P-AAA framework along with its primary entities and interfaces.

- Dmitry Tairov, Ivan Ganchev, Máirtín O'Droma (University of Limerick, Ireland). Ideas on a third-party authentication, authorization and accounting framework and associated signaling scenarios for a ubiquitous consumer wireless world. TD(11)011. URL: http://cost-winemo.org/tds.html. This paper was presented the 3rd meeting of European Science Foundation’s ‘COoperation in the field of Science and Technology research action on Wireless Networking for Moving Objects, WiNeMO, COST IC0906 [65], February 15, 2011, Riga, Latvia. The presentation described business model motivation for the emergence of the 3P-AAA infrastructure along with technical details of the framework design, IMS integration concerns, signalling and HAC handover concepts.

- Dmitry Tairov, Ivan Ganchev, Máirtín O'Droma (University of Limerick, Ireland). Third-Party AAA Framework and Signaling in UCWW [50]. This paper was accepted for the upcoming IEEE 7th International Conference on Wireless Communications, Networking and Mobile Computing, September 23-25, Wuhan, China. URL: http://www.wicom-meeting.org/2011/. This paper looks at the design of the 3P-AAA signalling protocol and investigates what currently existing signalling protocols could be used as a foundation of the signalling infrastructure.

- Dmitry Tairov, Ivan Ganchev, Máirtín O'Droma (University of Limerick, Ireland). Signaling messages and AVPs for 3P-AAA framework [53]. This paper was accepted for the upcoming IEEE 5th International Conference on Next Generation Mobile Applications, Services and Technologies, September 14-16, 2011, Cardiff, Wales. URL: http://www.ngmast.com/. Based on the work related to the anticipated signalling scenarios envisioned for the 3P-AAA framework, this paper looks at the requirements of each signalling interface and outlines the 3P-AAA signalling protocol stack along with new protocol messages and their corresponding attributes.
REFERENCES


ABSTRACT

Third-Party Authentication, Authorization and Accounting Framework for Ubiquitous Consumer Wireless World

Dmitry Tairov

This thesis proposes a new approach to the management of the Authentication, Authorization and Accounting (AAA) function that forms a core part of many service provider networks. The principle idea outlined is to move this function under the supervision of the trusted Third Parties and independent of the Access Network Providers. This change would provide for additional flexibility through enabling users to switch their network providers depending on their current needs and the required quality of service levels. The key issue addressed in this thesis is the development of the signaling framework for the Third-Party AAA, which is an integral entity of the Ubiquitous Consumer Wireless World (UCWW) [1, 2] project.

A review of the currently existing Business Models and Technologies is performed in the introducing chapters of the thesis. The key issue here is to investigate what currently existing technologies and protocols could be used to provide the base for the development of the 3P-AAA. Some of the signaling protocols along with security features are already implemented by a number of the network providers and can be inherited by the 3P-AAA. These features include signaling protocols like Diameter and PANA, as well as security features provided by the Extensible Authentication Protocol (EAP) and the X.509 Certificates.

Based on the researched material the 3P-AAA framework is described along with its corresponding entities and interfaces. Based on the discussion of the possible use scenarios and the requirements drawn from them, the 3P-AAA signaling protocol messages and novel Attribute-Value Pairs (AVPs) are outlined. The concluding chapter of the thesis aims to outline the implementation related issues that include the possible software protocol stacks and the simulation tools.

The ideas related to the 3P-AAA design outlined in this thesis have also been disseminated through presentations at international research conference meetings, namely Globe Forum Dublin and European Cooperation in Science and Technology Wireless Networking for Moving Object (WiNeMO) meeting. Various other aspects have been described in the IEEE conference paper publications within the upcoming 7th International Conference on Wireless Communications, Networking and Mobile Computing and the 5th International Conference on Next Generation Mobile Applications, Services and Technologies.
DECLARATION

I hereby declare that I am the sole author of this Master Thesis. I authorize University of Limerick to lend this Thesis to other institutions or individuals for the purpose of academic research.

I further authorize University of Limerick to reproduce this Master Thesis by photocopying or other means, in total or part, at the request of other institutions or individuals for the purpose of academic research.

Dmitry Tairov
ACKNOWLEDGEMENTS

I would like to thank my research supervisors, Dr Ivan Ganchev and Dr Máirtín ÓDroma, for their help and guidance. I am very thankful for the opportunity given to undertake the postgraduate studies especially in the difficult economic times present today.

On top of that I would like to express special gratitude to the Irish Research Council for Science, Engineering and Technology (IRCSET) for their financial support.
LIST OF FIGURES

Figure 1: Generic AAA Architecture ................................................................. 8
Figure 2: EAP Packet Format ............................................................................. 9
Figure 3: EAP Pass Through ............................................................................ 10
Figure 4: EAP over LAN .................................................................................. 11
Figure 5: User Certificate signing ................................................................... 12
Figure 6: 3-Way Authentication Procedure .................................................... 13
Figure 7: PANA functional components ........................................................... 14
Figure 8: IMS Architecture ............................................................................ 17
Figure 9: SIP Call Session .............................................................................. 19
Figure 10: RADIUS Message Format ............................................................... 23
Figure 11: Diameter Relay Agent .................................................................... 25
Figure 12: Diameter Redirect Agent ................................................................. 26
Figure 13: Diameter Translation Agent ............................................................. 27
Figure 14: Diameter Header ............................................................................ 27
Figure 15: AVP Header .................................................................................... 28
Figure 16: 3P-AAA framework ....................................................................... 35
Figure 17: Session outline .............................................................................. 39
Figure 18: Authentication and Authorization (Online Charging) ...................... 40
Figure 19: Authentication and Authorization (Offline Charging) ...................... 42
Figure 20: Service Delivery (Online Charging) ................................................ 44
Figure 21: Service Delivery (Offline Charging) ............................................... 46
Figure 22: Session Termination (Online Charging) .......................................... 48
Figure 23: Session Termination (Offline Charging) .......................................... 49
Figure 24: Abrupt Session Termination ............................................................ 50
Figure 25: ANP Re-Authentication and Re-Authorization (Online Charging) .... 51
Figure 26: ANP Re-Authorization Failure (Online Charging) ............................ 52
Figure 27: Successful Credit Replenishment .................................................. 54
Figure 28: Unsuccessful Account Replenishment .......................................... 55
Figure 29: Failover (ANP terminates session) .................................................. 58
Figure 30: Failover (ANP continues granting services) .................................... 59
Figure 31: User Triggered HAC (Online Charging) .......................................... 63
Figure 32: TSP/VASP Triggered HAC (Online Charging) ................................ 65
Figure 33: User triggered HAC with TSP change ......................................... 66
Figure 34: TSP HAC signalling (Online Charging) ......................................... 67
Figure 35: Access to teleservice(s) through different ANPs ............................ 68
Figure 36: Multiple ANP session ................................................................... 69
Figure 37: Value Added Services framework .................................................. 71
Figure 38: Service Delivery Chaining Example .............................................. 72
Figure 39: Service Delivery Chaining ............................................................... 73
Figure 40: Chained Service Session Termination ............................................ 74
Figure 41: 3P-AAA and IMS integration .......................................................... 75
Figure 42: 3P-AAA signalling protocol stack ................................................. 79
LIST OF TABLES

Table I: Base Diameter message codes .................................................................28
Table II: VAS classification (Balasubramanian et al.) .............................................70
Table III: Comparing signalling protocols ...............................................................77
Table IV: 3P-AAA signalling messages ....................................................................79
# LIST OF ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2G</td>
<td>Second Generation</td>
</tr>
<tr>
<td>3G</td>
<td>Third Generation</td>
</tr>
<tr>
<td>3GPP</td>
<td>3rd Generation Partnership Project</td>
</tr>
<tr>
<td>AAA</td>
<td>Authentication, Authorization and Accounting</td>
</tr>
<tr>
<td>ABC&amp;S</td>
<td>Always Best Connected and Served</td>
</tr>
<tr>
<td>ACE</td>
<td>Adaptive Communication Environment</td>
</tr>
<tr>
<td>ADA</td>
<td>Advertisement, Discovery and Association</td>
</tr>
<tr>
<td>AKA</td>
<td>Authentication and Key Agreement</td>
</tr>
<tr>
<td>ANI</td>
<td>Application-to-Network Interface</td>
</tr>
<tr>
<td>ANP</td>
<td>Access Network Provider</td>
</tr>
<tr>
<td>ASM</td>
<td>Application Specific Module</td>
</tr>
<tr>
<td>AVP</td>
<td>Attribute Value Pair</td>
</tr>
<tr>
<td>AuC</td>
<td>Authentication Centre</td>
</tr>
<tr>
<td>C&amp;B</td>
<td>Charging and Billing</td>
</tr>
<tr>
<td>CAMEL</td>
<td>Customized Applications for Mobile Network Enhanced Logic</td>
</tr>
<tr>
<td>CBM</td>
<td>Consumer-centric Business Model</td>
</tr>
<tr>
<td>CDMA</td>
<td>Code Division Multiple Access</td>
</tr>
<tr>
<td>CDR</td>
<td>Charging Detail Records</td>
</tr>
<tr>
<td>CHAP</td>
<td>Challenge-Handshake Authentication Protocol</td>
</tr>
<tr>
<td>CSCF</td>
<td>Call/Session Control Function</td>
</tr>
<tr>
<td>DECT</td>
<td>Digital Enhanced Cordless Telecommunication</td>
</tr>
<tr>
<td>E2E HAC</td>
<td>End to End Hot Access Change</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>EAPOL</td>
<td>EAP over LAN</td>
</tr>
<tr>
<td>EDGE</td>
<td>Enhanced Data rates for GSM Evolution</td>
</tr>
<tr>
<td>EIR</td>
<td>Equipment Information Register</td>
</tr>
<tr>
<td>EP</td>
<td>Enforcement Point</td>
</tr>
<tr>
<td>FA</td>
<td>Foreign Agent</td>
</tr>
<tr>
<td>FSM</td>
<td>Finite State Machine</td>
</tr>
<tr>
<td>GNU</td>
<td>GNU’s not Unix</td>
</tr>
<tr>
<td>GPRS</td>
<td>General Packet Radio Service</td>
</tr>
<tr>
<td>GSM</td>
<td>General System for Mobile communication</td>
</tr>
<tr>
<td>HA</td>
<td>Home Agent</td>
</tr>
<tr>
<td>HAC</td>
<td>Hot Access network Change</td>
</tr>
<tr>
<td>HLR</td>
<td>Home Location Register</td>
</tr>
<tr>
<td>HMIP</td>
<td>Hierarchical Mobile IP</td>
</tr>
<tr>
<td>HSS</td>
<td>Home Subscribe Service</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>IANA</td>
<td>Internet Assigned Number Authority</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronic Engineers</td>
</tr>
<tr>
<td>IETF</td>
<td>International Engineering Task Force</td>
</tr>
<tr>
<td>IMS</td>
<td>IP Multimedia Subsystem</td>
</tr>
<tr>
<td>IM-SSF</td>
<td>IP Multimedia Service Switch Function</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LRF</td>
<td>Location Retrieval Function</td>
</tr>
<tr>
<td>MAHO</td>
<td>Mobile Assisted HandOver</td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest algorithm 5</td>
</tr>
<tr>
<td>MIP</td>
<td>Mobile IP</td>
</tr>
<tr>
<td>MMD</td>
<td>MultiMedia Domain</td>
</tr>
<tr>
<td>MVNO</td>
<td>Mobile Virtual Network Operator</td>
</tr>
<tr>
<td>NASREQ</td>
<td>Network Access Server Requirements</td>
</tr>
<tr>
<td>NGN</td>
<td>Next Generation Networks</td>
</tr>
<tr>
<td>NNI</td>
<td>Network-to-Network Interface</td>
</tr>
<tr>
<td>OCF</td>
<td>Online Charging Function</td>
</tr>
<tr>
<td>OSA</td>
<td>Open Service Access</td>
</tr>
<tr>
<td>OTT</td>
<td>Over The Top</td>
</tr>
<tr>
<td>PAA</td>
<td>PANA Authentication Agent</td>
</tr>
<tr>
<td>PaC</td>
<td>PANA Client</td>
</tr>
<tr>
<td>PAN</td>
<td>Personal Area Networks</td>
</tr>
<tr>
<td>PANA</td>
<td>Protocol for carrying Authentication for Network Access</td>
</tr>
<tr>
<td>PAP</td>
<td>PPP Authentication Protocol</td>
</tr>
<tr>
<td>PDA</td>
<td>Personal Digital Assistant</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>POSIX</td>
<td>Portable Operation System for Unix</td>
</tr>
<tr>
<td>PPP</td>
<td>Point-to-Point Protocol</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial In User Service</td>
</tr>
<tr>
<td>RFC</td>
<td>Request for Commence</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Shamir &amp; Adelman</td>
</tr>
<tr>
<td>SAX</td>
<td>Simple API for XML</td>
</tr>
<tr>
<td>SCTP</td>
<td>Stream Control Transmission Protocol</td>
</tr>
<tr>
<td>SE</td>
<td>Service Equipment</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Terminal Access Controller Access-Control System Plus</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TRC</td>
<td>Telecommunication Research Centre</td>
</tr>
<tr>
<td>TSP</td>
<td>Teleservice Provider</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>UCWW</td>
<td>Ubiquitous Consumer Wireless World</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunication System</td>
</tr>
<tr>
<td>VASP</td>
<td>Value Added Service Provider</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Networks</td>
</tr>
<tr>
<td>WAP</td>
<td>Wireless Application Protocol</td>
</tr>
<tr>
<td>WBC</td>
<td>Wireless Broadcast Channels</td>
</tr>
<tr>
<td>WiMAX</td>
<td>Wireless Interoperability for Mobile Access</td>
</tr>
<tr>
<td>WiNeMO</td>
<td>Wireless Networking for Moving Objects</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
</tbody>
</table>
CONTENTS

Abstract .......................................................................................................................... i
Third-Party Authentication, Authorization and Accounting Framework for Ubiquitous Consumer Wireless World ......................................................... i
Declaration .................................................................................................................. ii
Acknowledgements .................................................................................................. iii
List of Figures .............................................................................................................. iv
List of Tables ............................................................................................................... v
List of Abbreviations ............................................................................................... vi
Chapter 1 ..................................................................................................................... 1
Introduction ................................................................................................................ 1
1.1 Introduction ......................................................................................................... 1
1.2 Business Models ................................................................................................ 2
  1.2.1 Mobile Virtual Network Operator (MVNO) Business Model ................. 2
  1.2.2 Two-Sided Telecoms Business Model .................................................... 2
  1.2.3 Over the Top (OTT) Business Model ...................................................... 3
  1.2.4 The “Freemium” Business Model ............................................................ 3
  1.2.5 The “Smart Pipe” Business Model ........................................................... 3
1.3 Research Objectives ........................................................................................... 3
1.4 Thesis Organization ............................................................................................ 4
1.5 Conclusion ............................................................................................................ 5
Chapter 2 ..................................................................................................................... 6
AAA and Security Frameworks ................................................................................ 6
2.1 Introduction ......................................................................................................... 6
2.2 Security Services ............................................................................................... 6
2.3 Generic AAA Architecture ................................................................................ 7
2.4 Extensible Authentication Protocol (EAP) Framework ..................................... 9
2.5 Public Key Infrastructure X. 509 Certificates Framework ............................. 11
  2.5.1 Authentication Procedure ....................................................................... 12
  2.5.2 Implementation Issues ............................................................................ 13
2.6 Protocol for carrying Authentication for Network Access (PANA) Architecture ........................................................................................................ 14
2.7 IP Multimedia Subsystem (IMS) Infrastructure ............................................. 15
   2.7.1 IMS Architectural Overview ................................................................. 16
2.8 Session Initiation Protocol Framework ....................................................... 18
2.9 Conclusion ..................................................................................................... 20
Chapter 3 ............................................................................................................ 21
AAA Protocols- RADIUS and Diameter ............................................................. 21
  3.1 Introduction .................................................................................................. 21
  3.2 Remote Authentication Dial-In User Service (RADIUS) ............................. 21
     3.2.1 RADIUS Message Format ................................................................. 22
     3.2.2 RADIUS Accounting ................................................................. 23
  3.3 Diameter ..................................................................................................... 24
     3.3.1 Diameter nodes and agents ............................................................. 25
     3.3.2 Diameter Messages ........................................................................... 27
     3.3.3 Diameter Peers .................................................................................. 29
     3.3.4 Error Handling .................................................................................. 29
     3.3.5 Diameter Sessions ............................................................................. 30
     3.3.6 Accounting ......................................................................................... 31
     3.3.7 Diameter Credit Control ................................................................. 31
     3.3.8 Diameter’s Evolution ......................................................................... 32
  3.4 Conclusion .................................................................................................. 33
Chapter 4 ............................................................................................................ 34
3P-AAA Framework ............................................................................................. 34
  4.1 Introduction ................................................................................................. 34
  4.2 Entities ......................................................................................................... 35
  4.3 3P-AAA Interfaces ....................................................................................... 36
     4.3.1 Interface ‘a’ ....................................................................................... 36
     4.3.2 Interface ‘b’ ....................................................................................... 37
     4.3.3 Interface ‘c’ ....................................................................................... 37
  4.4 3P-AAA Scenarios ....................................................................................... 38
     4.4.1 Basic Signalling Scenarios ................................................................. 38
     4.4.2 HAC Related Scenarios ................................................................. 60
     4.4.3 Novel 3P-AAA Scenarios ................................................................. 65
  4.5 3P-AAA and IMS integration ................................................................. 74
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.6 Conclusion</td>
<td>75</td>
</tr>
<tr>
<td>Chapter 5</td>
<td>77</td>
</tr>
<tr>
<td>3P-AAA Signalling</td>
<td>77</td>
</tr>
<tr>
<td>5.1 Introduction</td>
<td>77</td>
</tr>
<tr>
<td>5.2 3P-AAA Protocol Stack</td>
<td>77</td>
</tr>
<tr>
<td>5.3 Messages and AVPs</td>
<td>79</td>
</tr>
<tr>
<td>5.3.1 Messages over Interface ‘a’</td>
<td>80</td>
</tr>
<tr>
<td>5.3.2 Messages over Interface ‘b’</td>
<td>85</td>
</tr>
<tr>
<td>5.3.3 Messages over Interface ‘c’</td>
<td>87</td>
</tr>
<tr>
<td>5.4 3P-AAA AVPs</td>
<td>94</td>
</tr>
<tr>
<td>5.5 Conclusion</td>
<td>97</td>
</tr>
<tr>
<td>Chapter 6</td>
<td>98</td>
</tr>
<tr>
<td>Implementation Issues</td>
<td>98</td>
</tr>
<tr>
<td>6.1 Protocol Stacks</td>
<td>98</td>
</tr>
<tr>
<td>6.1.1 OpenDiameter</td>
<td>99</td>
</tr>
<tr>
<td>6.1.2 OpenBlox</td>
<td>100</td>
</tr>
<tr>
<td>6.1.3 JDiameter</td>
<td>100</td>
</tr>
<tr>
<td>6.1.4 Cpana</td>
<td>101</td>
</tr>
<tr>
<td>6.2 Simulation Issues</td>
<td>101</td>
</tr>
<tr>
<td>6.3 Conclusion</td>
<td>102</td>
</tr>
<tr>
<td>Chapter 7</td>
<td>103</td>
</tr>
<tr>
<td>Conclusions and Future Work</td>
<td>103</td>
</tr>
<tr>
<td>Research outcomes published to date</td>
<td>106</td>
</tr>
<tr>
<td>References</td>
<td>108</td>
</tr>
</tbody>
</table>
CHAPTER 1

INTRODUCTION

1.1 Introduction

Ubiquitous Consumer Wireless World (UCWW) is aimed at the creation of the novel wireless environment. What makes UCWW different from the currently existing frameworks is a different business model approach. UCWW proposes to move away from the currently deployed Subscriber-based Business Model (SBM), where every user needs to subscribe to a service in order to use it, to the Consumer-centric Business Model [1]. The way to achieve this is seen though the move of the Authentication, Authorization and Accounting (AAA) function under the supervision of the trusted Third Party Providers. This strategic innovation would enable consumers to gain access to the network and teleservices without the need for the long-term subscription with the corresponding service providing bodies.

Wireless telecommunication industry has seen many stages of development in the last few decades. These can be traced from the deployment of the analog networks all the way to the creation of the wireless 3G networks that are currently introduced to the wide public around the world, and with plans for evolving into 4G wireless communications at an advanced stage. Traditionally wireless networks were concerned with two types of services: voice and data. What we currently experience is a major shift towards all-IP networks and demand for higher speed and quality of service (QoS). However, it should be noted that the advances in the telecommunication industry have mostly been technology driven. UCWW and the deployment of the CBM aim to create a more liberal and open environment that in turn would be stimulation to the emergence of the new business opportunities.

The rest of this chapter looks at some of the currently existing business models and trends. It also focuses on the general research objectives of the thesis which aim at the discussion of the principle milestones in the development of the 3P-AAA framework. The last section of this introductory chapter describes the outline of the thesis.
1.2 Business Models

This section looks briefly at the business models currently employed in the industry [3]. The traditional business model heavily relies on voice revenues. However, currently there is a lot of demand for data services and more personified packaged service bundles. Operators are faced with stiff competition from Over the Top (OTT) applications and content providers such as Facebook, Twitter etc. New business models should enable the move of the decision-making power towards customers and application providers and away from the traditional service providers.

1.2.1 Mobile Virtual Network Operator (MVNO) Business Model

In this business model wireless network service providers lease their networks to other carriers. Thus Mobile Virtual Network Operators (MVNO) cannot participate in the provision of the spectrum to customers but they can generate revenues through innovating, operating and selling mobile services. While traditionally for wireless network provider provision of spectrum is seen as a primary task and provision of additional services is only an auxiliary source of revenue, for MVNO service provision becomes a specialization and they are able to target certain niche markets. The resurgence of MVNOs is based on the new business model emphasizing delivery of total solutions with wireless as part of the package. An example is the free Amazon Whispernet content service bundled with a Kindle reading device [4].

1.2.2 Two-Sided Telecoms Business Model

With development of the wireless broadband networks, operators will have the option of not only bundling voice, broadband data and media content, but also to leverage their assets to link upstream customers to downstream customers. Upstream companies may include industries and communities providing services to downstream customers i.e. traditional wireless consumers where operator plays role of the middle man. To move into two-sided telecom business model, wireless operators need to:

- Be more consumer orientated
- Modernize their platforms to support different charging models and to control exposure to their assets
- Learn from success of companies such as Facebook, Google and Apple which were successful at providing their application store solutions and support
1.2.3 Over the Top (OTT) Business Model

Over the last few years there has been an increase in the competition between “over-the-top” service providers versus the carriers. The term “over-the-top” refers to the provision of services on top of the internet connection independent of the subscriber’s ISP. The problem with this thriving business model is that OTT providers are dispersed and their service platforms are not standardized.

1.2.4 The “Freemium” Business Model

This model focuses on the provision of a free basic service where charging is only applied to the premium content. Basic services might not necessarily be web applications but also content such as software, games etc. This model is very well suited for innovative services that the people are not familiar with. There is a greater incentive to try out new things if they are free of charge.

1.2.5 The “Smart Pipe” Business Model

This term refers to an operator’s network which leverages existing or unique service capabilities as well as the operator’s own customer relationships to provide value beyond data connectivity [5]. In other word it is an ability of an operator to offer added value to unique types of services.

As can be seen from the examples of the business models mentioned above, the Subscriber-based Business Model (SMB) dominates the telecommunication market.

1.3 Research Objectives

A key role in the AAA management is proposed to be given to a 3P-AAA not integral to the traditional wireless communications. This alternative is attractive in that it separates out this administration and management of consumers’ one-stop-shop accounting system and the various business agreements with other parties from the business of supplying a wireless access network service [1, 2]. All types of teleservice providers (TSPs) and access network providers (ANPs) will be able to offer their services to mobile users through the business agreements each and all will have with third-party AAA service providers (3P-AAA-SPs), who become the central players in UCWW. Mobile users will have arrangements with one or more 3P-AAA-SP, just as they have one or more credit cards, and similarly through this entity will receive periodic itemized bills for all services used. The mobile users’ choice of 3P-AAA-SPs at any time for any service will be dictated by decision processes similar to those in deciding which credit card to use for a particular bill.
CBM’s 3P-AAA infrastructure follows guidelines for the NGN systems[3], as it centralizes customer and product data within 3P-AAA framework. 3P-AAA would create a better environment for the enforcement of converged charging since all the charging and billing takes place within 3P-AAA and not within numerous access and teleservice providers. Overall, it would create a stimulating environment for consumer centric service personalization.

The following can be considered the main objectives of the research described in this thesis:

- Creation of a foundational infrastructure that would enable the core AAA functionality to be placed in the hands of ‘non-communications third-party management companies’. Success here will lead to a radical re-structuring of how wireless communication services may be created, deployed, delivered and paid for and to a real possibility to satisfy the legitimate modern consumer expectation of being able to move back and forth readily among access networks/providers at any time for any and all services. Furthermore, such an attribute is a major contribution towards the realisation of the ‘always best connected and best served’ (ABC&S) capability for the consumers [1, 2].

- Investigation of how the newly created infrastructure can be integrated with technologies and frameworks widely deployed throughout the industry today. These include evaluation of the interfaces and signalling infrastructure employed by 3GPP IP Multimedia Subsystems (IMS). IMS presents an interesting case study since it allows for the deployment of third-party Value Added Services.

- Development of a 3P-AAA interface architecture - three main application-layer interfaces are foreseen: Mobile User ↔ ANP/TSP (a); Mobile User ↔ 3P-AAA-SP (b); and ANP/TSP ↔ 3P-AAA-SP (c).

- Development of a 3P-AAA signalling protocol based on the evaluation of the possible interaction scenarios and signalling requirements - the IETF Diameter protocol is considered as a main candidate to carry the 3P-AAA signalling. However, adjustments of it for 3P-AAA will be required. The application autonomy would also help the process of developing the standards for the three indicated interfaces. In support of this the application capability range would include all necessary functionality with defined messages for 3P-AAA, purchaser transactions, mobility, user privacy, etc. [1, 2]

1.4 Thesis Organization

The rest of this thesis is organized as follows:
• Chapter 2 looks at the concepts and protocols related to the AAA. It also briefly looks at the architecture of the IP Multimedia Subsystems (IMS) that can serve as an example study case of the AAA framework.
• Chapter 3 focuses primarily on the two examples of the AAA signalling protocols—RADIUS and Diameter.
• Based on the ideas expressed in the previous chapters, chapter 4 draws an outline of the 3P-AAA framework. Principle interfaces and signalling scenarios describe the types of interactions that could be handled by this framework.
• Chapter 5 concentrates on the definition of the signalling messages and corresponding Attribute-Value Pairs (AVPs) based on the requirements outlined in chapter 4.
• Chapter 6 discusses implementation issues that need to be overcome in order to successfully implement outlined framework.
• Chapter 7 concludes this thesis.

1.5 Conclusion

This introductory chapter aims to introduce the key motives for the emergence of the proposed framework. Some of the key concepts related to UCWW, such as the difference between the SBM and the CBM are outlined. In order to demonstrate the contrast between the two business models, some of the currently existing and deployed business model variations of the SBM are given. A conclusion could be drawn from the description of the above-mentioned business models, that in general, there exists a need for new business opportunities among different service providers in order to continue generating revenues. Thus the emergence of the 3P-AAA framework could be beneficial not only to the consumer, but also to the service providers as it will create a stimulating environment for the emergence of these opportunities. At last, the principle objectives of the thesis are outlined that will be covered in more detail in the proceeding chapters.
CHAPTER 2

AAA AND SECURITY FRAMEWORKS

2.1 Introduction

Authentication, Authorization and Accounting is commonly used in telecommunication infrastructure to identify users, control access to data and keep track of the resources used. Thus the aim of this chapter is to provide an overview of the technical aspects involved in the provision of an adequate AAA service. Since 3P-AAA would require to carry sensitive data, security is one of the central issues. This chapter looks at the definition of the security services along with two security frameworks that will be considered for the 3P-AAA: the Extensible Authentication Protocol (EAP) and the X.509 Certificates. Additionally, the interfaces employed by the 3P-AAA would have to carry their data by means of some signalling protocol. Two signalling protocols, Session Initiation Protocol (SIP) and PANA, will be studied in order to see if these protocols or some of their features may be adapted by the 3P-AAA framework. In order to see how some of these technologies and protocols are being employed in the industry, the Third Generation Partnership IP Multimedia Subsystems (IMS) framework will be discussed as a study case example.

2.2 Security Services

A good AAA systems should be concerned with provision of reliable security services that would benefit not only the service provider but also an end-user. A number of security services can be identified [6]:

- Authentication-The authentication service is concerned with assuring that a communicating party is authentic, i.e., that it is what it claims to be. Authentication is accomplished via the claimant's presentation of an identifier and its corresponding credentials to the verifier. Examples of types of credentials are passwords, one-time tokens, digital certificates, and phone numbers (calling/called).
- Authorization (Access Control) - In the context of network security, access control is the ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.
• Accounting- Accounting refers to the tracking of the consumption of network resources by users. This information may be used for management, planning, billing, or other purposes. Real-time accounting refers to accounting information that is delivered concurrently with the consumption of the resources. Batch accounting refers to accounting information that is saved until it is delivered at a later time. Typical information that is gathered in accounting is the identity of the user, the nature of the service delivered, when the service began, and when it ended.

• Data Integrity- Integrity can apply to a stream of messages, a single message, or selected fields within a message. A connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent, with no duplication, insertion, modification, reordering, or replays. The destruction of data is also covered under this service. On the other hand, a connectionless integrity service, one that deals with individual messages without regard to any larger context, generally provides protection against message modification only.

• Data Confidentiality- Confidentiality is the protection of transmitted data from passive attacks. With respect to the content of a data transmission, several levels of protection can be identified. The broadest service protects all user data transmitted between two users over a period of time. The other aspect of confidentiality is the protection of traffic flow from analysis. This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility.

• Non-Repudiation- Non-repudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

2.3 Generic AAA Architecture

Because of the significance of the AAA infrastructure and widespread popularity of the Internet and Multimedia services, special group within the IRTF (Internet Research Task Force) was created- AAAarch Research Group- to continue research in the area of architectural development. This group ceased to exist in 2004; nonetheless some significant work has been carried out, including generation of RFC2903 “Generic AAA Architecture” [7]. It proposed an AAA infrastructure composed of generic AAA servers communicating via a standard protocol. The server activity is general; however, different applications requiring AAA services will have unique needs. Following components could be outlined:
- Application Specific Module (ASM) - ASMs are capable of handling even complex authentication and authorization requests. They interact with the generic server. The server will know to which ASM to forward a request and will receive an answer from the ASM whether the user is authenticated or not.

- Service Equipment (SE) - The SE provides a service to a user such as access to the internet.

- Authorization Event Log - This database is used to log the authorizations happening in the server. These events are used for accounting purposes. To account a user, the server has to know for example how long it used the authorized service. Authorization to a request can also be made depending on an event that occurred in the past.

- Policy Repository - This database contains the available services that can be authorized to a request.

The generic server interactions are shown in the Figure 1. The generic AAA server receives request, processes and forwards request to AAA server by means of common protocol. For the other interactions other protocols will be used.

![Figure 1: Generic AAA Architecture](image)

RFC2903 also stresses the importance of investigation of the management rules in the multi-domain AAA infrastructure because the future success is highly dependent on the manageability of this infrastructure.
Other work carried out by the AAAarch Research Group was concerned with Authorization Framework [8]. Based on the research of the group a memo was published containing Authorization Requirements [9]. The document outlines the main requirements for the creation of AAA protocol and provides separate guidelines under the following headings: security of authorization information, application proxying, trust models, administration etc.

In the next sections we look at some of the protocols that are actively being used in the AAA infrastructure. The examples of the older authentication protocols are PAP (PPP Authentication Protocol) [10] and CHAP (Challenge-handshake Authentication Protocols) [11]. These two protocols are commonly used in Point-to-Point communication links. In PAP the password is transmitted over without any protection which makes it vulnerable to the eavesdropping attacks. CHAP is a bit more secure and uses MD5 checksum hash to provide integrity during the three-way handshake authentication process. These protocols were commonly used in the wired connections; however, in the wireless environment, where more threats are present due to the open nature of communication, there is a common demand for better and more secure protocols.

### 2.4 Extensible Authentication Protocol (EAP) Framework

A number of Layer2 security protocols exist, but EAP [12] is probably one of the most commonly used. An interesting thing about EAP is that it is not really an authentication protocol, but rather a transport framework that supports a number of authentication mechanisms or methods. These methods can offer different levels of security. For example EAP-MD5 offers minimum level of security as it uses MD5 hashing algorithm that is considered weak and vulnerable to dictionary attacks. On the other hand EAP-TLS [13] is a strong method that uses PKI (Public Key Infrastructure). EAP-TLS is not commonly used in the wireless environment as public-key cryptography has a high level of overhead and demands more processing power than symmetric cryptographic methods.

The EAP framework is peer-to-peer and is based on request/response model. The format of EAP packet is shown in Figure 2:

<table>
<thead>
<tr>
<th>Code</th>
<th>Identifier</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data...</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 2: EAP Packet Format
Packet is 32 bit wide with Code field occupying 8bits. There are only 4 codes defined for EAP: 1- Request, 2- Response, 3-Success, 4-Failure.

EAP can operate in pass-through mode when authenticator has to query the authentication server. In this case EAP peer sends request to the authenticator that in turn forwards query to the authentication server. In the diagram below an EAP Peer sends a request to the authentication server via Authenticator (Access Point or Network Access Server). EAP message is encapsulated into Point-to-Point Protocol (PPP), 802.1X or Protocol for carrying Authentication for Network Access (PANA) in the Peer-Authenticator transaction and over an AAA protocols between Authenticator and the Authentication Server.

![Figure 3: EAP Pass Through](image)

IEEE 802.1X standard, also known as EAPOL (EAP over LAN), is aimed to provide authentication mechanism for port-based network access control that makes use of 802 LAN infrastructure by using EAP methods. In this case if a client using 802.11 wants to access Internet services it sends a request through Access Point that later forwards EAP messaged to AAA server over the LAN as shown in Figure 4.
2.5 Public Key Infrastructure X. 509 Certificates Framework

Public Key Infrastructure X.509 Certificates can be used in variety of applications that use web browsing, e-mail, user authentication services etc. The protocol outlined in RFC3280 [14] describes basic mechanism of operation. The protocol itself does not dictate use of a specific public key algorithm; however, its RFC document’s examples use RSA. Initially, user has to obtain a X.509 Certificate from a trusted Certificate Authority (CA).  Below are listed fields included in the X.509 Certificate [6]:

- **Version**: Differentiates among successive versions of the certificate format; the default is version 1. If the Issuer Unique Identifier or Subject Unique Identifier is present, the value must be version 2. If one or more extensions are present, the version must be version 3.
- **Serial number**: An integer value, unique within the issuing CA, that is unambiguously associated with this certificate.
- **Signature algorithm identifier**: The algorithm used to sign the certificate, together with any associated parameters. Because this information is repeated in the Signature field at the end of the certificate, this field has little, if any, utility.
- **Issuer name**: name of the CA that created and signed this certificate.
- **Period of validity**: Consists of two dates: the first and last on which the certificate is valid.
- **Subject name**: The name of the user to whom this certificate refers. That is, this certificate certifies the public key of the subject who holds the corresponding private key.
- **Subject's public-key information**: The public key of the subject, plus an identifier of the algorithm for which this key is to be used, together with any associated parameters.
• Issuer unique identifier: An optional bit string field used to identify uniquely the issuing CA in the event the X.500 name has been reused for different entities.

• Subject unique identifier: An optional bit string field used to identify uniquely the subject in the event the X.500 name has been reused for different entities.

• Extensions: A set of one or more extension fields. Extensions were added in version 3 in order to enable addition of optional fields that may be deemed important by some organizations implementing security.

• Signature: Covers all of the other fields of the certificate; it contains the hash code of the other fields, encrypted with the CA's private key. This field includes the signature algorithm identifier.

Figure 5 shows the steps taken to sign user’s certificate. As can be seen from the diagram, the authenticity of user is provided by the CA. Also, no other party than CA can modify certificate without this being detected. In cases when the security has been compromised or validity period of the certificate has expired, it is responsibility of the corresponding CA to revoke this certificate.

![Diagram of User Certificate signing](image)

Figure 5: User Certificate signing

2.5.1 Authentication Procedure

Authentication procedure that uses X.509 Certificates can be used in order to provide mutual authentication of the communicating parties. These includes 2-Way and 3-Way authentication. Figure 6 below shows steps and information necessary to accomplish the latter:
• First message is sent signed with A’s private key, includes timestamp, nonce generated by A, ID of the corresponding party and a session key encrypted with B’s public key
• B responds with a message containing its own timestamp and nonce, A’s ID, A’s nonce that was sent in the previous message and a matching session key encrypted with A’s public key
• The last steps is specific to 3-Way authentication and is only required in cases when synchronization clocks are not available

Furthermore it should be noted that when the procedure takes place in the real world there is an additional level of protection provided by the Transport Layer Security (TLS) [15] that handles transport of the authentication messages.

![Figure 6: 3-Way Authentication Procedure](image)

2.5.2 Implementation Issues

PKI X.509 infrastructure presents a fairly good security framework, nonetheless, there are issues related to the implementation of the infrastructure. One of the weaknesses comes from the fact that the framework does not impede implementation and utilization of weak security methods. For example, the use of previously widely accepted MD5 algorithm for hashing may produce security vulnerability due to the flaws in the algorithm’s design and its relative weakness. A whole range of issues surface related to specific vendor implementations. Infrastructure’s security model is based on the reliability and competence of the Certificate Authority. The question that might be posed is “who guards the guards” as some CAs might abuse trust through adoption of feeble practices. It is reported that often when X.509 Certificate expires, CA will renew subscription, but without the issue of new key-pair thus encouraging a prolonged key exposure. The root of the problem resides in the poor control of the service providing CAs [16].
2.6 Protocol for carrying Authentication for Network Access (PANA) Architecture

PANA [17] is a relatively new protocol that was created to enable to perform network-layer authentication independent of the underlying link-layer technology. PANA is a UDP-based EAP lower layer that runs between the EAP peer and the EAP authenticator (Figure 3). Since UDP (destination port 716) is used at the transport layer it is the responsibility of the protocol to retransmit lost or damaged messages, as UDP does not provide mechanisms for retransmission.

Figure 7 displays the main components of the architecture: PANA Client (PaC), PANA Authentication Agent (PAA), Enforcement Point (EP) and the Authentication Server.

- **PANA Client (PaC):** The PaC is the client implementation of PANA and resides on the node wishing to gain access to the network.
- **PANA Authentication Agent (PAA):** The PAA is the server implementation of PANA. It is the responsibility of PAA to interface with PaC in order to authenticate and authorize network access.
- **Enforcement Point (EP):** EP controls access to network resources. All the network traffic directed at PaC will have to pass through EP. The EP uses non-cryptographic and cryptographic filters to check data packets. In case if cryptographic access control is used, a security association needs to be established between EP and PaC. Once association is established per-packet security is enabled to provide integrity protection.
- **Authentication Server (AS):** Authentication Server makes decision on whether the end system can be authenticated or not. AAA protocol is used on the communication link between PAA and AS.

The following stages can be distinguished in the functioning of the protocol:
1. Authentication and authorization phase—once communication was started by either PAA or PaC, the actual exchange of EAP messages occurs. Once this phase is over PAA knows whether the PaC is authorized or not.

2. Access phase—during this stage PaC gains access to network and can send and receive IP traffic that passes through EP. It is also possible to send ping packets by PANA peer in order to verify that the session is still active.

3. Re-authentication—session can enter re-authentication stage, where current session’s lifetime is extended in case if re-authentication is satisfied. Otherwise session is terminated.

4. Session termination can be initiated by either of two parties: PaC or PAA.

PANA message codes have a general request/answer type of communication. The important data within the message is embedded in AVPs (Attribute-Value-Pairs). A protocol defines the following command codes:

- PANA-Client-Initiation (PCI)
- PANA-Auth-Request (PAR)
- PANA-Auth-Answer (PAA)
- PANA-Termination-Request (PTR)
- PANA-Termination-Answer (PTA)
- PANA-Notification-Request (PNR)
- PANA-Notification-Answer (PNA)

2.7 IP Multimedia Subsystem (IMS) Infrastructure

It is only logical that the next step in the development of telecommunication networks would be integration of the wireless services where users will see transition to the all-IP services. Some of the principle entities of the converged Next Generation Network (NGN) architecture include:

- Business Support Systems (BSS) that focus on management of business relationships with customer and include such tasks as billing, payment processing, revenue management etc.
- Operation Support Systems (OSS) provide support for network management including provisioning, troubleshooting, inventory.
- Service Delivery Platforms (SDP) support creation, deployment, execution and management of one or several classes of services. SDP also provides a managed 3rd party access to network services through web services standard.
- 3GPP IP Multimedia Subsystems (IMS) is an architectural framework for delivering IP multimedia services. The biggest achievement of IMS is decoupling of the application and control planes from the underlying access technologies.
With the current move to new 3G technology mobile operators commonly try to conform to the standards and interfaces specified by 3GPP/3GPP2. Both of these organizations are not privately owned bodies but rather associations of telecommunication groups that set as their main goal to define a number of technical specifications that later would be globally applicable in the telecommunication industry. 3GPP (3rd Generation Partnership Project) defines technical specification for technologies that have evolved from the GSM technology. A number of task groups exist within 3GPP each one charged with specific architecture-related development tasks.

Another organization that executes similar tasks is 3GPP2. This organization is charged with development of technical specifications for 3rd Generation network devices that are based on the Code Division Multiple Access (CDMA) access technology that is very widely deployed in the North America and Japan.

Deployment of 3G networks heralds creation of improved telecommunication infrastructure. Arrival of IMS (IP Multimedia Subsystem) was a major step taken for the provision of IP Multimedia services to the users of mobile networks. IMS is a subsystem of 3GPP; its equivalent in 3GPP2 is called the MultiMedia Domain (MMD). Both frameworks perform the same function i.e. provide access to IP multimedia services to mobile users and share similar architectural design. As far as the project is concerned, we are primarily interested in the signalling interfaces and functional entities related to the AAA functionality. Thus we will take a closer look at what functional elements the 3P-AAA framework could inherit from the 3GPP IMS architecture.

2.7.1 IMS Architectural Overview

The primary entities of the diagram describe architectural layout of the IMS. As can be seen in Figure 8, 3GPP separates Transport and IMS planes from the Service plane. This creates a level of abstraction that permits development of the new services independent from the lower levels.

- CSCF (Call Session Control Function) - this entity can be of four different types: Proxy, Interrogating, Emergency and Serving. CSCF can be seen as an intermediary body in communication between the mobile user and the Home Subscriber Server (HSS). When User Equipment (UE) first tries to access IMS Proxy CSCF (P-CSCF) is responsible for finding and associating this user and Serving CSCF. P-CSCF sits on the pass of all signalling messages and can inspect every message. Another important function carried out by this entity is authentication of the UE. Additionally, it is responsible for generation of charging records. Interrogating CSCF (I-CSCF) is primarily used for roaming scenarios as it is responsible for locating the corresponding HSS for the subscriber in question. Emergency CSCF (E-CSCF) shall be able to retrieve geographical location information from the Location Retrieval
Function (LRF) in the case that the geographical location information is not available and is required [18]. Serving CSCF (S-CSCF) is the central entity of the signalling plane and is typically located within the home network. It is also an enforcement point of the network.

Figure 8: IMS Architecture

- **HSS (Home Subscriber Server)** - a central piece in this architecture as it can be seen as a master database. This database stores user identity information, all the security vectors, network access information and user profile information. HSS is responsible for generation of information that is used for user authentication and integrity checks. Other entities such as AuC (Authentication Centre), EIR (Equipment Identity Register) and HLR (Home Location Registered) logically would reside within HSS.

- **AS (Application Server)** – support for three different types of application servers are provisioned within the framework: Session Initiation Protocol (SIP) Application server, Open Service Access (OSA) Application server and Customer Application for Mobile network Enhanced Logic (CAMEL) IP Multimedia Service Switching Function (IM-SSF) server. These servers offer value-added services and can reside either inside the network or in the 3rd party location. Application servers interact with S-CSCF using SIP protocol. In case if the SIP Application server resides within the home network, it can access HSS directly through Sh Diameter interface. One peculiarity of the OSA Application server is that it does not interact directly with IMS but does so through OSA Server Capability Server. IM-SSF provides transition for legacy services.
Two signalling protocols can be emphasized from the given architectural outline: SIP and Diameter. Operations related to the policy control, subscriber information access, charging and billing are handled by the 3GPP-extended Diameter protocol. User-interaction session control and application service interactions are handled by SIP. The Third-party Value Added Service Provider (VASP) communicates with the underlying network by means of OSA/Parlay interface. Creation of the OSA API is a joint effort between ETSI (European Telecommunication Standardization Institute), 3GPP and The Parlay Group [19].

2.8 Session Initiation Protocol Framework

Session Initiation Protocol (SIP) is an application layer protocol used for session set up and control. It has been defined by RFC3261 [20]. This application level protocol that in structure resembles that of Hyper Text Transfer Protocol (HTTP) is currently widely deployed in a number of applications. As outlined in the specification document, SIP provides the following set of services:

- User location: determination of the end system to be used for communication;
- User availability: determination of the willingness of the called party to engage in communications;
- User capabilities: determination of the media and media parameters to be used;
- Session setup: "ringing", establishment of session parameters at both called and calling party;
- Session management: including transfer and termination sessions, modifying session parameters, and invoking services.

It can run on top of User Datagram Protocol (UDP) and Transmission Control Protocol (TCP), as well as newer Stream Control Transport Protocol (SCTP). The basic operation of the SIP can be described by the discovery and session setup between different network entities as well as negotiation of the session parameters. SIP is commonly used for control of multimedia streams. It uses Session Description Protocol (SDP) [21] to set up a multimedia session by listing session requirements. This mechanism can be used for provision of the appropriate QoS levels.

This type-text protocol uses a set of request/response messages to communicate between different entities of the infrastructure. The common requests are:

- REGISTER: Used by a User Agent to indicate its current IP address and the URLs for which it would like to receive calls.
- INVITE: Used to establish a media session between user agents.
- ACK: Confirms reliable message exchanges.
- CANCEL: Terminates a pending request.
- **BYE**: Terminates a session between two users in a conference.
- **OPTIONS**: Requests information about the capabilities of a caller, without setting up a call.
- **PRACK (Provisional Response Acknowledgement)**: PRACK improves network reliability by adding an acknowledgement system to the provisional Responses (1xx). PRACK is sent in response to provisional response (1xx).

Figure 9 below shows an example of the session setup between two SIP User Agents. The session is torn down once media transfer is finished. As can be seen from the diagram, the response format is similar to the HTTP response format:

- **Provisional (1xx)**: Request received and being processed.
- **Success (2xx)**: The action was successfully received, understood, and accepted.
- **Redirection (3xx)**: Further action needs to be taken (typically by sender) to complete the request.
- **Client Error (4xx)**: The request contains bad syntax or cannot be fulfilled at the server.
- **Server Error (5xx)**: The server failed to fulfil an apparently valid request.
- **Global Failure (6xx)**: The request cannot be fulfilled at any server.

![Figure 9: SIP Call Session](image)

SIP inherited some of its authentication methods from HTTP. However, this Digest Access Authentication method only allows the server to authenticate the user but
does not support the reverse operation of authenticating the server to the user. Since SIP is so widely spread, a number of security extensions were developed for it. Typically an X.509 Certificate exchange takes place during TLS setup that requires use of TCP; however, there is an extension that allows an X.509 Certificate exchange over SCTP [22]. That means that X.509 Certificate based authentication may be performed to mutually authenticate the Mobile User and the access network element.

An additional functionality of SIP is that it can provide location management and presence related services. This ability is especially valuable in the modern environment where user may have several communication devices.

2.9 Conclusion

The principle goal of this chapter was to make an introduction to the technical aspects related to the AAA framework. Going from the general to the specific, the security services and the generic AAA architecture were discussed first followed by the more specific description of the EAP and the X.509 Certificates. The X.509 Certificates are discussed in a greater detail, since the certificate exchange mechanism is quiet suitable for the implementation of the mutual authentication within the 3P-AAA framework. The signalling protocols were introduced in order to see what features can be inherited by the 3P-AAA signalling protocol. Since PANA was design specifically for the provision of the authentication features, these features could be integrated into the 3P-AAA signalling. On the other hand, SIP provides a wider array of session control services, including the authentication, and is more suitable for handling the multimedia sessions. As a matter of fact, SIP and Diameter, which will be discussed in the next chapter, are the two primary signalling protocols employed by the IMS framework. Finally, in order to see how some of the technical aspects and features can be combined together, IMS was presented as a real world example of a functional framework.
CHAPTER 3

AAA PROTOCOLS- RADIUS AND DIAMETER

3.1 Introduction
The authentication protocols looked at in the previous chapter carry out Authentication/Authorization functions however they do not monitor the usage of network resources. Implementation of the “true” AAA protocol should not only perform Authentication and Authorization, but also Accounting where careful records of the network/service consumptions should be taken. This chapter focuses on two widely used AAA protocols: RADIUS and its descendent Diameter. Both of these protocols provide the AAA functionality, however, Diameter is newer and was developed to overcome the weaknesses of its predecessor and thus will be discussed in greater detail. With the introduction of the Diameter Base protocol a number of supporting applications has emerged to provide additional functionality and supporting features. The principle purpose of this chapter is to demonstrate that the rich set of features provided by the Diameter protocol would allow it to become the foundation of the 3P-AAA signalling.

3.2 Remote Authentication Dial-In User Service (RADIUS)

RADIUS [23] protocol is a true AAA protocol as it is concerned with Authentication, Authorization and Accounting features. RADIUS is very commonly used by Internet Service Providers (ISPs) to manage access to network resources. One of the disadvantages of RADIUS is its poor scalability as it does not provide any congestion control mechanisms.

RADIUS uses client-server model of communication. A Network Access Server (NAS) acts as a client of RADIUS. It contacts the RADIUS server. In order to improve the scalability issue RADIUS server network can be organized in the hierarchical manner, where in case if the authorization request cannot be resolved at the local RADIUS server, the request will be forwarded to the next server up the hierarchy chain. When client wishes to authenticate using RADIUS, it creates an “Access-Request” with such attributes as user’s name, password, ID of the client etc. In order to provide integrity of the message the password is hidden using the RSA MD5.
Once the RADIUS server receives the request, it validates the sending client. A request from a client for which the RADIUS server does not have a shared secret must be silently discarded. If the client is valid, the RADIUS server consults a database of users to find the user whose name matches the request. The user entry in the database contains a list of requirements which must be met to allow access for the user. This always includes verification of the password, but can also specify the client(s) or port(s) to which the user is allowed access.

The server might challenge the client. In this Access-Challenge response a pseudorandom number, also known as nonce will be send. Using the pre-shared key client will encrypt the number and return it to the server. RADIUS uses UDP for transport and two ports have been assigned to the RADIUS protocol: 1812 for RADIUS Authentication and port 1813 for RADIUS Accounting. However, prior to the official assignment of port by the IANA (the Internet Assigned Number Authority), ports 1645 and 1646 were used. These ports are still in use for backward compatibility. Designers of the protocol considered that UDP was a better option for AAA as it provided less overhead and simplified the server implementation due to the stateless nature of the protocol.

As well as that, in comparison to PANA, where keep-alive messages are being exchanged in order to verify that the session is still active, RADIUS discourages the use of keep-alive messages since they don’t provide any additional useful information. It is suggested that other protocols, such as Simple Network Management Protocol (SNMP) should be used for these purposes.

Because RADIUS uses MD5 hashing that is considered to be cryptographically weak [24], it is recommended to use other security protocols such as IPsec [25, 26] or TLS [15].

### 3.2.1 RADIUS Message Format

As seen in Figure 10, the message is 32bit wide. The following codes are identified in the authentication protocol:

- 1 Access-Request
- 2 Access-Accept
- 3 Access-Reject
- 4 Accounting-Request
- 5 Accounting-Response
- 11 Access-Challenge
- 12 Status-Server(experimental)
- 13 Status-Client(experimental)
- 255 Reserved
The identifier field is only one octet and is used to match requests and responses. In addition each message can carry a number of attributes that relate information between the client and the server.

![Figure 10: RADIUS Message Format](image)

### 3.2.2 RADIUS Accounting

When a client is configured to use RADIUS Accounting, at the start of service delivery it will generate an Accounting Start message describing the type of service being delivered and the user it is being delivered to, and will send that to the RADIUS Accounting server, which will send back an acknowledgement that the message has been received. At the end of service delivery the client will generate an Accounting Stop message describing the type of service that was delivered and optionally statistics such as elapsed time, input and output octets, or input and output messages. It will send that to the RADIUS Accounting server, which will send back an acknowledgement that the message has been received.

It is recommended that the client continue attempting to send the Accounting-Request packet until it receives an acknowledgement, using some form of back off algorithm. If no response is returned within a length of time, the request is resent a number of times. The client can also forward requests to an alternate server or servers in the event that the primary server is down or unreachable. An alternate server can be used either after a number of tries to the primary server fail, or in a round-robin fashion. If the RADIUS accounting server is unable to successfully record the accounting packet it must not send an Accounting-Response acknowledgment to the client.

The format of the messages for RADIUS accounting is the same as for authentication where Attributes would be specifically defined for accounting purposes.
3.3 Diameter

RADIUS is a very popular protocol and is widely used by the operators. However, due to some shortcomings of the RADIUS original design and overall changes in the requirements due to the development in telecommunication industry, a better and more reliable protocol was needed. Therefore it is envisaged that the newly developed AAA Diameter protocol will replace RADIUS in the near future.

The Diameter base protocol provides the minimum requirements needed for an AAA protocol as described in [28]. The base protocol may be used by itself for accounting purposes only, or it may be used with other Diameter application.

There are a number of reasons why Diameter is seen as the successor of RADIUS, the major one being a more careful design and consideration for future development. Diameter was designed to be extensible. Extensibility can be achieved through addition of new application specific command codes and Attribute Value Pairs (AVPs). Among other advantages of Diameter, the following may be listed:

- Diameter provides more reliable transport by running over TCP and SCTP, in comparison to UDP transport of RADIUS.
- Unlike RADIUS which does not describe any failover mechanism, Diameter defines failover algorithms and the corresponding state machine.
- As far as transport-layer security is concerned, it’s a requirement for Diameter applications to support IPsec or TLS.
- Diameter base protocol provides agent support, thus a Diameter peer can be a Redirect, Proxy or Relay agent.
- Diameter possesses better roaming support. Even though the concept of proxying exists in RADIUS, due to poor transportation security and lack of auditability, it is vulnerable to the man-in-the-middle attacks. Diameter with its features allows for better roaming and scalability.
- Diameter supports error handling and capacity negotiations

Diameter is designed as a peer-to-peer architecture, and a Diameter node can act as a client or as a server depending on the network implementation. Apart from the Redirect, Proxy and Relay agents, Translation agent is supported by the Diameter protocol to provide backward compatibility with RADIUS.

The base Diameter protocol concerns itself with capabilities negotiation, how messages are sent and how peers may eventually be abandoned. The base protocol also defines certain rules that apply to all exchanges of messages between Diameter nodes.

Communication between Diameter peers begins with one peer sending a message to another Diameter peer. The set of AVPs included in the message is determined by a
particular Diameter application. One AVP that is included to reference a user's session is the Session-Id.

The initial request for authentication and/or authorization of a user would include the Session-Id. The Session-Id is then used in all subsequent messages to identify the user's session. The communicating party may accept the request, or reject it by returning an answer message with the Result-Code AVP set to indicate an error occurred. The specific behaviour of the Diameter server or client receiving a request depends on the Diameter application employed.

The session state (associated with a Session-Id) must be freed upon receipt of the Session-Termination-Request, Session-Termination-Answer, expiration of authorized service time in the Session-Timeout AVP, and according to rules established in a particular Diameter application.

Diameter base protocol support both TCP and SCTP transport protocols and is allocated port 3868. It is specified in the base protocols that while client can support either of the two transport methods, the agents and the servers must support both.

### 3.3.1 Diameter nodes and agents

The typical entries within the protocol are clients and servers, however for scalability and backward compatibility other nodes were introduced into the system: relay agents, proxy agent, redirection agent and translation agent.

- **Relay Agents** - Relays forward requests and responses based on routing-related AVPs and realm routing table entries. Figure 11 demonstrates basic use of a relay agent. Since relays do not make policy decisions, they do not examine or alter non-routing AVPs. As a result, relays never originate messages, do not need to understand the semantics of messages or non-routing AVPs, and are capable of handling any Diameter application or message type. Since relays make decisions based on information in routing AVPs and realm forwarding tables they do not keep state on NAS resource usage or sessions in progress.

![Figure 11: Diameter Relay Agent](image-url)
• Proxy Agents – Similar to relays, proxies forward request and response messages and their operational diagram is equal to that of Figure 11. However, proxies also make policy decisions related to resource usage and provisioning. This is typically accomplished by tracking the state of NAS devices. While proxies typically do not respond to client Requests prior to receiving a Response from the server, they may originate Reject messages in cases where policies are violated. As a result, proxies need to understand the semantics of the messages passing through them, and may not support all Diameter applications.

• Redirection Agents - Rather than forwarding requests and responses between clients and servers, redirect agents refer clients to servers and allow them to communicate directly (Figure 12). Since redirect agents do not sit in the forwarding path, they do not alter any AVPs transiting between client and server. Redirect agents do not originate messages and are capable of handling any message type, although they may be configured only to redirect messages of certain types, while acting as relay or proxy agents for other types. As with proxy agents, redirect agents do not keep state with respect to sessions or NAS resources.

![Diagram of Diameter Redirect Agent](image-url)
Translation Agents - A translation agent is a stateful Diameter node that is used to provide backward compatibility with legacy protocols. It performs protocol translation between Diameter and another AAA protocol, such as RADIUS (Figure 13).

![Figure 13: Diameter Translation Agent](image)

### 3.3.2 Diameter Messages

All the information between different Diameter nodes is exchanged by means of messages that have specific structure. The outline of the Diameter header is given in Figure 14. Each message carries command code that specifies the action that peer is currently performing, but the real data is carried by the AVPs of the message.

![Figure 14: Diameter Header](image)

Command Flags filed is 8 bit wide. Only the first four bits are assigned in the base protocol. These are Request, Proxiable, Error and Potentially Retransmitted Message bits. It must be noted that if the Request bit is set, i.e. message is a request message then the Error bit must be cleared.

Hop-by-Hop Identifier field is used for matching request and reply messages. End-to-End Identifier is used to detect duplicate messages in case of failover.
In the Diameter base protocol 14 command code messages were defined listed in Table I:

Table I: Base Diameter message codes

<table>
<thead>
<tr>
<th>Message Name</th>
<th>Abbreviation</th>
<th>Command Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abort-Session-Request</td>
<td>ASR</td>
<td>274</td>
</tr>
<tr>
<td>Abort-Session-Answer</td>
<td>ASA</td>
<td>274</td>
</tr>
<tr>
<td>Accounting-Request</td>
<td>ACR</td>
<td>271</td>
</tr>
<tr>
<td>Accounting-Answer</td>
<td>ACA</td>
<td>271</td>
</tr>
<tr>
<td>Capabilities-Exchanging-Request</td>
<td>CER</td>
<td>257</td>
</tr>
<tr>
<td>Capabilities-Exchanging-Answer</td>
<td>CEA</td>
<td>257</td>
</tr>
<tr>
<td>Device-Watchdog-Request</td>
<td>DWR</td>
<td>280</td>
</tr>
<tr>
<td>Device-Watchdog-Answer</td>
<td>DWA</td>
<td>280</td>
</tr>
<tr>
<td>Disconnect-Peer-Request</td>
<td>DPR</td>
<td>282</td>
</tr>
<tr>
<td>Disconnect-Peer-Answer</td>
<td>DPA</td>
<td>282</td>
</tr>
<tr>
<td>Re-Auth-Request</td>
<td>RAR</td>
<td>258</td>
</tr>
<tr>
<td>Re-Auth-Answer</td>
<td>RAA</td>
<td>258</td>
</tr>
<tr>
<td>Session-Termination-Request</td>
<td>STR</td>
<td>275</td>
</tr>
<tr>
<td>Session-Termination-Answer</td>
<td>STA</td>
<td>275</td>
</tr>
</tbody>
</table>

As well as that, the Diameter Base protocol defines a number of AVPs that would be quiet common in the AAA type of application. It can be said that it is AVPs that carry the “real” data in the given protocol.

Each AVP has an AVP code that can be found in the AVP header (Figure 15), which uniquely identifies it. AVP numbers from 1 to 255 are reserved for backward compatibility with RADIUS.

AVP Flags provide additional information on how attributes must be handled. The ‘r’ bits should be set to 0 and are reserved for future applications. The ‘P’ bit indicates need for end-to-end security.
‘M’ bit stands for Mandatory and all Diameter implementations are required to support these AVPs. AVPs with this bit cleared are informational.

‘V’ bit is a Vendor-Specific bit and indicates whether the optional Vendor-ID is present.

Apart from the Basic Data formats, such as OctetString, Integer and Float, AVPs can support derived data formats. It is also allowed to use AVP values of type ‘Grouped’ where Data field is a sequence of AVPs. This allows for AVP nesting, when one Grouped AVP contains another Grouped AVP within.

3.3.3 Diameter Peers

Even though a Diameter node can have multiple peer connections sometimes it is not economical to establish connection to all of them. At a minimum Diameter node must have an established connection with two peers per realm, these peers are called primary and secondary peer. Secondary peer is used in case if the connection with primary peer has failed. Additional connections can be established if the need for them arises.

An important enhancement of Diameter is its peer discovery capabilities. Before a connection can be established between peers, they must exchange the Capabilities Exchange messages. In case if no common applications or common security was discovered, the peers should disconnect transport layer connection. It is also important to note that CER and CEA messages must not be proxied, redirected or relayed.

Given the nature of the Diameter protocol, it is recommended that the transport failures be detected as soon as possible. Detecting such failures will minimize the occurrence of messages sent to unavailable agents, resulting in unnecessary delays, and will provide better failover performance. The Device-Watchdog-Request and Device-Watchdog-Answer messages are used to proactively detect transport failures.

The communication between peers in Diameter follows a specific State Machine described in section 5.6 of [27]. This State Machine is used to open, close, failover, probe, and reopen transport connections. The watchdog messages are used to verify that the connection is still active.

3.3.4 Error Handling

Errors that occur in the Diameter fall into two categories: protocol and application errors. Protocol errors occur at the base protocol level. On the other hand application
errors generally occur due to the problems associated with a function of the specific Diameter application.

Result-Code AVP values that are used to report protocol errors must only be present in answer messages where ‘E’ bit is set. Typically Result-Code AVP describes the error that the Diameter node encountered and can be used for debugging purposes.

Error code of Diameter is similar to the semantics of the HTTP protocol. The first digit of the return code will identify the type of error:

- 1xxx Informational
- 2xxx Success
- 3xxx Protocol Errors
- 4xxx Transient Failures
- 5xxx Permanent Failures

Only the errors that fall into Protocol Errors category should have ‘E’ bit set in the answer message. The difference between Transient and Permanent Failures is that the former signifies that the request could not be satisfied at this time, but may be successful in the future, while the latter signifies that the request should not be attempted again.

### 3.3.5 Diameter Sessions

The Diameter Base protocol can provide two types of services to applications. First type involves the authentication and the authorization, and can optionally make use of the accounting. Second only makes use of the accounting.

When authentication and/or authorization takes place, a user sends request to the server. This request contains a Session-Id AVP. All subsequent messages that belong to the same session must contain this matching Session-Id AVP.

Because authentication/authorization messages are largely application specific, the authorization requests are not included in the base protocol. However, base protocol defines messages that are used for session termination. Session termination messages can be initiated by either Diameter client or server. Session-Termination-Request or Abort-Session-Request commands will be used in this case. When application makes use of only Accounting services, the Session-Id AVP still would be used, however, session termination will be signalled by issuing an accounting stop message.

Base protocol contains a set of finite state machines that must be observed by all Diameter implementations. Separate state machines exist for Authorization and Accounting services. There are four different authorization session state machines supported in the Diameter base protocol. The first two describe a session in which the server is maintaining session state, indicated by the value of the Auth-Session-State AVP (or its absence). One describes the session from a client perspective, the
other from a server perspective. The second two state machines are used when the server is stateless. Here again, one describes the session from a client perspective, the other from a server perspective.

### 3.3.6 Accounting

The Diameter Accounting protocol is based on a server directed model with capabilities for real-time delivery of accounting information. The server directed model means that the device generating the accounting data gets information from either the authorization server (if contacted) or the accounting server regarding the way accounting data shall be forwarded. Several fault resilience methods have been built in to the protocol in order minimize loss of accounting data in various fault situations and under different assumptions about the capabilities of the used devices. Due to the purpose of the accounting protocol a real-time transfer of data is a requirement, it needs to be fulfilled in order to perform credit limits checks.

Some of Diameter mechanisms are used to overcome small message loss and temporarily network failures. It is a requirement for a Diameter client to implement failover mechanism described in the base protocol. It is also recommended to use non-volatile storage for accounting records until the acknowledgment from the Diameter server was received. This mechanism can be used when network congestion cause delays or when Diameter server is temporarily down.

Base protocol has four types of accounting message AVPs: EVENT_RECORD, STOP_RECORD, START_RECORD and INTERIM_RECORD. INTERIM_RECORD may be used in cases when client accesses services for a lengthy period of time, where timing interval can be set and may also depend on Re-Authorization and Re-Authentication timer. EVENT_RECORD indicates one-time event (event where start and stop occur simultaneously) and carry all the relevant information. Since it is possible for one client to access multiple services within one session, the Diameter messages must contain AVPs that use the same session-ID but will use different sub session-IDs.

### 3.3.7 Diameter Credit Control

Since the time of the development of the original protocol, a number of other applications were implemented using Diameter protocol targeting specific services, such as Diameter SIP Application for session management, Diameter EAP Application implementing EAP framework, Diameter Credit Control Application [29] etc. Credit Control application’s significance is that it enables the service provider to implement online real-time charging with credit reservation. Many interface used in 3GPP for charging and billing use Credit Control Application [30]. In comparison to the base protocol Credit Control Application only defines two
new messages. These messages are Credit Control Request and Answer. Since the signalling strength of the protocol rests with the data encoded in AVPs, this application defines a great number of new AVPs specific to the credit control task.

The application differentiates between two distinct modes of charging: session based and one-time events. Session based charging performs multiple interrogations of the Credit Control server during an on-going session. Since some scenarios may include possibility of access of multiple services per user session, sub-session charging is also facilitated. One-time event was created to accommodate request that do not require multiple interrogations and could be satisfied by a single request/answer message. These scenarios include direct debiting, credit checks and price enquiries.

3.3.8 Diameter’s Evolution

Diameter was created to serve as a successor to RADIUS. There are plenty of examples of wide adaptation of this protocol in the industry. Regardless of the careful architectural design and wide spread adoption, some issues have surfaced only during implementation and deployment of the protocol. Evolving standards have created different interpretations and implementation that lead to incompatibilities between vendors [31].

Some flaws have been found related to the protocol design. For example, the initial information exchange between peers that helps to establish a connection is not clearly specified in the RFC3588 and its interpretation may only be deduced from the state machines. The establishment of communication will be influenced by the list of the supported vendor identifiers. The problem here emerges when the corresponding end-to-end nodes support the same list of vendor but the intermediary nodes participating in the routing do not.

A lot of problems encountered are due to inappropriate setting of the M(andatory)-flag. This flag is used inside AVP to state that this AVP has to be supported by the receiving node. Generally, there is confusion between the ABNF defining the set of AVPs used in a Diameter command for the particular Diameter Application and the setting of the M-bit of an AVP for this same application.

Based on the protocol deployment experiences and in order to solve interoperability issues, Diameter Maintenance and Extensions (DIME) Technical Working group came up with new version of protocol that is currently under discussion. RFC3588bis document claims full backward compatibility with the original RFC3588 [32]. Here are some of the principle changes outlined within RFC3588bis:

- Deprecated the use of Inband-Security AVP for negotiating transport level security. New version of Diameter will establish TLS on the well-known secure port prior to exchange of traffic
- Deprecated the exchange of CER/CEA messages in the open state. It is assumed that the capabilities exchange in the open state will be described in more detail in a separate specification.

- Simplified security requirements. Use of secure transport is still mandatory; however, TLS will become the primary method of security traffic with IPsec being a secondary alternative. The support for end-to-end security framework has also been deprecated.

- The restriction concerning the support of accounting for all Diameter application is removed, as it does not make sense for some applications.

- Other small fixes address removal of obsolete types, fixes to command ABNFs, fixes to the state machine etc.

- Routing fixes are made through specification of what information can be used for making general routing decision. A separate internet draft is dedicated to Diameter routing optimizations [33].

### 3.4 Conclusion

This chapter has looked at the two principal AAA signalling protocols currently employed in the industry. Even though both protocols provide similar functionality, Diameter has more advanced features which make it more suitable and reliable for the purposes of this thesis. Also, Diameter was designed to be extensible and a number of new Diameter based applications has emerged after deployment of the Base protocol. These include Accounting and Credit Control applications that could be used to provide the offline and the online charging. Apart from the growing amount of the Diameter based applications, the Base protocol itself evolves and is currently going through a revision, aimed to remove some of the ambiguities and the original design flaws. Since the behaviour expected from the 3P-AAA signalling protocol introduces new features and scenarios that are not catered for in the original Diameter Base protocol, the Diameter 3P-AAA signalling protocol would have to define new messages and attributes in order to facilitate these salient features.
CHAPTER 4

3P-AAA FRAMEWORK

4.1 Introduction

As has been mentioned previously, the design of the 3P-AAA framework is one of the central issues in the development of the UCWW. This framework is conceived on the idea that the 3P-AAA service providers would be responsible for management and maintenance of the AAA features which would be separated from the provision of the access- and tele- services. The communication between different parts of the framework will take place through the new interfaces. The principle challenge is not only the through design of these interfaces but also their standardization. Overcoming the challenge of global standardization of the 3P-AAA interfaces would give a strong incentive to further development of the open 3P-AAA infrastructure. Due to the resilience requirements and sensitivity of the data traversing these interfaces, a careful examination of each interface’s functionality should be performed. The challenge is that the creation of 3P-AAA would produce new forms of interactions and scenarios that have not been previously seen. For example, regarding the decoupling of provision of teleservices from that of access communication services, the interaction with third-party VASP should be direct through one of these interfaces. This is quite different from the way third-party VASP services are being accessed now, i.e. through home access network where a Service Level Agreement (SLA) exists between home network and third-party VASP. Thus, prior to the actual service deployment, VASP has to be plugged into IMS Open Service Access (OSA) or other Service Delivery Platform. The principle tasks of these entities is that they perform accounting and charging tasks, and provide information regarding the network resources that can be accessed by the third-party VASP. Within 3P-AAA these entities can be replaced by interface interactions since charging and accounting will be serviced by the 3P-AAA service providers and network resources access can be advertised through other entities of UCWW i.e. Wireless Broadband Channels (WBC) and Advertisement, Discovery and Associations (ADA) agents [34].

This chapter sets out to cover the principle ideas outlined by the 3P-AAA framework. Sections that follow will outline the main entities and interfaces envisioned. In order to gather requirements for the 3P-AAA signalling, different forms of interactions between the 3P-AAA entities will be described in the section
covering signalling scenarios. This section covers a lot of material and looks at the interactions that take place during different stages of the access. Scenarios involving the 3P-AAA specific Hot Access-network Change (HAC) handover will look at the cases when more than one service provider is available in the area. Some of the novel forms of interactions that would be possible in the 3P-AAA environment are also outlined. The final section of this chapter will outline the possibility of the co-existence of the 3P-AAA with other technologies such as 3GPP IMS.

4.2 Entities

Figure 16 [35] shows the three principle interfaces envisioned for the 3P-AAA framework along with the principle functional elements of the framework.

- **Mobile User (MU)** - this entity is the typical end-consumer of the services provided by the other entities of the framework. MU will receive great flexibility and wider range of services through exchange of subscriptions with Internet Service Providers, Mobile Operators etc. for subscription with a third-party AAA provider. MU is an abstraction for generic user and can physically be represented by mobile phones, laptops or in some scenarios described later as another service provider.

- **Access Network Provider (ANP)** - 3P-AAA aims at separating provision of access from the provision of services. This entity represented as an ANP domain in the diagram, can be composed of numerous physical servers. Typically it would have an access server that would perform authentication and authorization and would be the first point of contact with a user. Since during provision of access, media and control stream will be flowing through this entity, it will perform policy enforcement and metering functions. ANP will also have a back-end server that would be connected to the 3P-AAA-SP
for the purposes of communication of the relative data. When offline charging is involved, it may not be necessary to contact 3P-AAA server during authentication and authorization stage, hence, back-end server may handle these decisions based on the authentication procedure results.

- TeleService Provider (TSP) - this entity is responsible for the provision of non-access services. Just as ANP it would be composed of an access server and a back-end server connected to the 3P-AAA service provider. During provision of a teleservice, there is a certain dependence on the state of the session between MU and ANP, since transport is required for the service provision. This state will be monitored by the signalling interfaces.

- Value Added Service Provider (VASP) - this entity is responsible for the provision of value-added services. In telecommunication industry, Value Added Services (VAS) term encompasses a wide range of services and may be defined as any type of a non-core service available to the end user. Since provision of phone calls can be considered as a primary core service, VAS includes such commonly used mobile technologies as SMS, MMS and GPRS. Currently most of the VAS are implemented and deployed by the mobile operators. As a result, in order to gain access to some VAS and applications, a mobile user first needs to create a service level agreement with a mobile operator.

- 3P-AAA-SP- this entity is the key element of the infrastructure. It is the vertex of the infrastructure’s communication charged with multiple critical tasks. The 3P-AAA-SP’s infrastructure must be secure, reliable and scalable. Hierarchic deployment of 3P-AAA servers could be a good strategy for the provision of scalability.

4.3 3P-AAA Interfaces

4.3.1 Interface ‘a’

This interface is responsible for the MU’s communication with the service providing entities, i.e. ANPs, TSPs, and VASPs. It is over this interface where a session with the service of interest is established and maintained. The aliveness of the session is monitored by the signalling messages. In case of events that might cause change in the session state, an informative update message is exchanged between communicating peers. When the mobile user has finished using the service, a session termination procedure would take place.

Security is a major concern for this interface, since it operates in the most vulnerable (i.e. wireless) environment in comparison to the other interfaces. Previously, as in Global System for Mobile Communication (GSM) networks, the authentication procedure between the mobile user and the network provider has been one-way only. However, nowadays wireless service providers can be easily spoofed
by malicious attackers. Taking this fact into consideration, it is important to perform a two-way authentication between communicating parties. 3P-AAA employs X.509 certificates for mutual authentication of peers. In order to provide strong authentication features, the three-way authentication option of X.509 should be employed. The benefit of the three-way authentication is that it puts less stringent requirements for time synchronization between different devices employed. In the 3P-AAA framework, the last (third) message carries also an authentication decision back to the party that initiated the authentication procedure.

4.3.2 Interface ‘b’

The primary purpose for this interface is to enable interaction between the mobile user and his/her 3P-AAA-SP. A number of diverse tasks can be attributed to this interface. The mobile user would be able to interact with his/her 3P-AAA account for purposes like checking the accounting information and possible profile settings interaction. Another key feature of the 3P-AAA framework is to provide accounting and billing transparency. Interacting with a multiple set of access- and teleservice providers, the mobile user has to be ensured that the charges applied by these diverse entities are indeed accurate. After each session termination procedure taking place, the mobile user issues a request to 3P-AAA-SP for Charging Detail Record (CDR) for the recently terminated session. The MU’s equipment can aggregate appropriate CDR information and calculate whether the charges applied have been accurate. In some scenarios where connection to the 3P-AAA-SP has been lost during an ongoing session, it might be appropriate for the service provider to store accounting data locally without service interruption and later forward updated data to the 3P-AAA server. Even in this case, the state machine has to ensure that the CDR data is still delivered to the end user.

4.3.3 Interface ‘c’

This interface performs vital task of providing important information for authorization, accounting and charging tasks. All entities of the 3P-AAA framework that provide services would be connected by means of ‘c’ interface to the 3P-AAA-SP server. Security is also an important issue for this interface but unlike interface ‘a’, entities communicating by means of interface ‘c’ share security association through initial subscription. Resilience of the interface is of paramount significance since it handles accounting and charging related streams of data. Thus it should be able to handle failover scenarios. This interface will also provide a flexible charging to the framework through adaptation of the online and offline charging capabilities. Online charging is synonymous to the idea of the prepaid services, where in order to access services first a credit check is performed on the user account and certain amount is debited or reserved. Online charging is performed in real-time and can
thus influence the session state. Offline charging is less stringent and does not require the credit control facilities. When offline charging is used the usage of resource is reported and charges are applied based on the amount of resources consumed. This kind of charging is less flexible and is typically used for the subscription-based services.

4.4 3P-AAA Scenarios

This section will look at some signalling scenarios employed in the 3P-AAA framework. Based on this scenarios and requirements for the interfaces, signalling protocol details will be drawn up. Scenarios outlined here may be decomposed into three primary categories: those not involving handover procedures, scenarios with Hot Access network Change (HAC) and some novel scenarios that could be facilitated by the 3P-AAA infrastructure.

4.4.1 Basic Signalling Scenarios

Figure 17 shows a typical scenario where Mobile User accesses some ANP/TSP/VASP resources. These interactions can be broken into three principle phases:

1) Initial phase- mutual authentication using the X.509 Certificates takes place followed by the authorization performed to ensure that the Mobile User has clearance to access requested services.

2) Access phase- access and use of resources. Prior to granting access, the availability of the credit on Mobile User’s account is checked. Depending on the implementation multiple credit control and accounting messages may be exchanges during the on-going session.

3) Terminating phase- this phase terminates sessions between different entities of the infrastructure. Also in order to provide better charging and credit control transparency Charging Detail Records are requested by Mobile User for every session.

4.4.1.1 Phase 1: Authentication and Authorization

Authentication can be accomplished between Mobile User and ANP/TSP/VASP without a query to the 3P-AAA server. This may be accomplished through the use of the X.509 Certificate Infrastructure. In order to provide strong authentication features and mutual authentication of entities, a 3-Way Authentication should be employed. The benefit of the 3-Way Authentication is that it puts less stringent requirements for time synchronization between different devices employed. Since 3-Way Authentication only requires 3 signalling exchanges between two peers and our
infrastructure is based on the request/response model, the last message response carries authentication decision back to the party that initiated the authentication procedure.

Even though authentication can take place without referral to the 3P-AAA server, when a request for resource usage is sent, the local ANP/TSP/VASP server will be queried whether the Mobile User has permission to access this resource. Depending on the charging implementation of the particular type of service, a credit control check will be performed in case if the online charging is used. Also since no assumptions should be made as to the geographical location of the 3P-AAA server and the level of the network congestion, Credit Control request should be sent by ANP/TSP/VASP towards the 3P-AAA server on the first round of the 3-Way Authentication procedure. This will allow to reduce the time delay and to have an authorization decision ready by the final round of the authentication procedure. Once authentication is accomplished, the decision of the authorization will be forwarded to

Figure 17: Session outline
the Mobile User notifying of the results of the authentication and authorization procedures.

Figure 18 displays a Mobile User who wants to get an access to an Access Network managed by the ANP1 and then to access some services provided by the TSP1. In both cases authentication and authorization procedures are performed.

- A Mobile User wants to access services provided by ANP1. A 3P-AAA-MU-Initiation message is sent towards ANP1 gateway. The address of ANP may be received via Wireless Billboard Channel (WBC) [34] service, DHCP server or can be manually configured. During this stage ANP1 gains knowledge of the MU’s identity.
- A 3P-AAA-Start-Request is issued by ANP1 on the reception of the initiation message. ANP1 issues Session ID for this session and forwards start request to MU. This Session ID will be contained within every signalling message exchanged during this session. In order to complete authentication procedure, the MU and the ANP need to exchange their corresponding X.509 Certificates. The ANP attaches its Certificate to the request message. X.509...
v3 Certificates allow inclusion of a number of private extensions to provide more flexible and optimized services.

- A 3P-AAA-Start-Answer is returned from Mobile User as an acknowledgement that it will continue participation in the session with the MU’s Certificate attached.
- Having received ANP’s Certificate, the MU can now complete the first step of the 3-Way Authentication procedure. The 3P-AAA-Auth-Request contains message that will include at minimum a timestamp, a nonce, an ID of ANP and a number of additional extension.
- A Credit-Control-Request message is sent towards the 3P-AAA server to verify that the MU has sufficient credit to access the ANP.
- Having MU’s Certificate at its disposal, the ANP1 can continue with the second step of the authentication procedure, extracting relevant information from the MU’s Certificate and sending a 3P-AAA-Auth-Answer towards MU containing a timestamp, nonce received previously from the MU as well as a nonce generated by the ANP1 itself, MU’s ID and a session key signed with MU’s public key.
- The 3P-AAA-Auth-Request completes the last step of the X.509 3-Way Authentication procedure. The intent of the third step is to address synchronization issue between devices. The information related to the authentication procedure includes return of the nonce previously generated by the ANP1 back to ANP1 for verification.
- Prior to completing the last step of the Authentication procedure, the ANP1 server waits for a Credit-Control-Answer message and makes authorization decision based on that message as well as on the identity of the user and the service requested.
- The MU receives the 3P-AAA-Auth-Answer message signalling the result of the authentication and authorization procedures.
- Once the ANP authentication and authorization is complete and both parties are satisfied with results, the MU repeats the above steps in order to complete TSP1 authentication. The message exchange between the MU and the TSP1 is similar.

Figure 19 describes interactions in case when the offline charging is performed by the system:

- A Mobile User wants to access services provided by theANP1. 3P-AAA-MU-Initiation message is sent towards ANP1 gateway. The address of the ANP may be received via Wireless Billboard Channel (WBC) service, DHCP server or can be manually configured. During this stage, the ANP1 gains knowledge of the MU’s IPv6 address.
- A 3P-AAA-Start-Request is issued by theANP1 on the reception of the initiation message. TheANP1 issues Session ID for this session and forwards start request to MU. This Session ID will be contained within every
signalling message exchanged during this session. In order to complete authentication procedure the MU and the ANP need to exchange their corresponding X.509 Certificates. The ANP attaches its Certificate to the request message. X.509 v3 Certificates allow inclusion of a number of private extensions to provide more flexible and optimized services.

Figure 19: Authentication and Authorization (Offline Charging)

- **3P-AAA-Start-Answer** is returned from the Mobile User as an acknowledgement that it will continue participation in the session with the MU’s Certificate attached.
- Having received ANP’s Certificate, the MU can now complete the first step of the 3-Way Authentication procedure. The **3P-AAA-Auth-Request** contains message that will include at minimum a timestamp, a nonce, an ID of ANP, optionally a session key signed with ANP’s public key and a number of additional extension.
Since the service requested uses the offline charging, no 3P-AAA solicitation takes place and the authorization decision made by the ANP1 is local, based on the authorization privileges and considerations of the network provider.

Having MU’s Certificate at its disposal, the ANP1 can continue with the second step of the authentication procedure, extracting relevant information from the MU’s Certificate and sending a 3P-AAA-Auth-Answer towards MU containing a timestamp, nonce received previously from the MU as well as a nonce generated by ANP itself, MU’s ID and session key signed with MU’s public key.

The 3P-AAA-Auth-Request completes the last step of the X.509 3-Way Authentication procedure. The intent of the third step is to address synchronization issue between devices. The information related to the authentication procedure includes return of the nonce previously generated by the ANP1 back to ANP1 for verification.

The MU receives the 3P-AAA-Auth-Answer message signalling the result of the authentication and authorization procedure.

Once ANP authentication and authorization is complete and both parties are satisfied with results, the MU repeats the above steps in order to complete the TSP1 authentication. The message exchange between the MU and TSP1 is similar.

4.4.1.2 Phase 2: Access Phase

The following scenario looks at the signalling that takes place when the Mobile User gets access to some service within ANP/TSP/VASP. Once the authentication and authorization process completes successfully, the Mobile User should be able to access the service requested. In case if the Mobile User is not aware of the charges applied for the requested service, the 3P-AAA-Price-Enquiry-Request/Answer messages may be exchanged between the Mobile User and the corresponding ANP/TSP/VASP.

Depending on the charging implementation of the ANP/TSP/VASP and type of the service accessed, multiple interrogations of the 3P-AAA server may be performed during the session. In case if access was authorized for multiple resources, Credit Control messages exchanged may belong to the same session but have different Sub-Session Ids.

Figure 20 shows the messages exchanged when the Mobile User is trying to access some services that implement online (real-time) charging. The following steps take place:
Prior to establishing association with ANP/TSP/VASP entities, the Mobile User may inquire about the charges applied for the services that the MU seeks. The 3P-AAA-Price-Enquiry-Request messages may be sent towards the corresponding ANP/TSP/VASP servers. Service ID as well as the IP addresses of ANP/TSP/VASP gateways may be received through the WBC service. The 3P-AAA-Price-Enquiry –Answer should contain full information regarding the charges applied.

Figure 20: Service Delivery (Online Charging)
• If after checking the price, the Mobile User is still interested in using the services offered by ANP/TSP/VASP, in order to gain access to the network a mutual authentication is performed between the MU and the ANP1 based on the X.509 Certificate Authentication. During this stage ANP1 will check availability of the credit on the MU’s account and will reserve certain amount of credit depending on the service in question.

• Having successfully accomplished authentication and authorization phase, the Mobile User gains access to the service, i.e. network coverage in this case. Since online charging offers a flexible charging and credit control framework, the 3P-AAA1 will maintain session and monitor use of the reserved credit. A number of intermediate updates will be exchanged between the 3P-AAA1 and the ANP1 servers.

• Once network coverage is available, the Mobile User may want to access certain teleservices. In order to do that, the mutual authentication takes place between the Mobile User and the corresponding TSP/VASP. During this phase the MU’s account will be checked and credit reserved for use of TSP/VASP’s service.

• If both, the ANP1 and the TSP1, authentication and authorization phases were successful, the Mobile User has gained access to the services. In typical scenario where session online charging is performed a number of intermediate Credit-Control-Request/Answer messages will be exchanged. These messages are usually triggered by some mid-service events such as updates about the amount of used units, requests for additional credit reservation etc.

• The Final Credit Control message exchanges takes place either when user has finished using services and notifies the corresponding ANP/TSP/VASP that he/she wishes to disconnect or when the reserved units were consumed and not replenished. Messages exchanged during this stage will be described in the next section.

Offline charging (Figure 21) does not implement credit monitor and control and only reports accounting data back to the 3P-AAA server. This type of charging infrastructure is typical of the subscriber services.

• The MU wants to access services offered by ANP/TSP/VASP. First, an inquiry is made about the prices and charges applicable. This information is delivered by means of 3P-AAA-Price-Enquiry-Request/Answer messages.

• The Mobile User goes through authentication stage in order to gain access to the ANP1’s service. Since for this scenario offline charging is implemented, the 3P-AAA server consultation and credit reservation is not performed.
• If the authentication and authorization were successful, the Mobile User can gain access to the access network. The ANP1 will start reporting accounting data to the 3P-AAA server.

• If the Mobile User is wishing to access some teleservices, he/she has to go through authentication and authorization process once more with the corresponding TSP/VASP.

• If authentication and authorization between the Mobile User and the TSP/VASP were successful, the Mobile User can start using a teleservice and the TSP/VASP will report accounting data to the 3P-AAA server.

• Depending on the implementation of the offline charging a number of intermediate accounting messages may be periodically exchanged followed by the final STOP message indicating termination of the accounting stream (shown in the next section).

Figure 21: Service Delivery (Offline Charging)
4.4.1.3 Phase 3: Termination Phase

During the termination stage different entities have to be notified of the session teardown. In a typical scenario when a user gains access to resources, makes use of them and finishes session, a 3P-AAA-Termination-Request is sent towards the ANP/TSP/VASP entity. Reception of the Termination Request signals final credit control/accounting. After terminating current session the Mobile User sends request to the 3P-AAA for its Charging Detail Record. Enabling this feature would provide for better charging and billing transparency as the Mobile User would be able to compare the usage claimed by the ANP/TSP/VASP versus her/his own records.

Figures 22 and 23 show interactions that take place during the session termination stages for online and offline scenarios, respectively.

- The Mobile User has finished and wants to terminate session. The 3P-AAA-Termination-Request message is sent towards the TSP/VASP.
- The TSP/VASP now knows that the Mobile User will not use any more resources and thus the final Credit Control (for online charging) or Accounting (for offline charging) messages may be exchanged to finalize data about the use of resources.
- The TSP/VASP can now tear down its session with the 3P-AAA server by exchanging Session-Termination-Request/Answer messages.
- Once session is torn down between the TSP/VASP and the 3P-AAA, a 3P-AAA-Termination-Answer is sent to the Mobile User signalling that the session can be safely terminated.
- After the session has been terminated, the Mobile User wants to ensure that the correct charges and use of resources statistics have been applied. Mobile User sends a 3P-AAA-CDR-Request directly to the 3P-AAA through ‘b’ interface. This message includes Session ID of recently terminated session.
- The 3P-AAA satisfies MU’s query by embedding its CDR within a 3P-AAA-CDR-Answer.
- If the MU does not issue any further requests for teleservice use and wishes to terminate its session with ANP it goes through the same steps as described above, this time addressing the ANP entity.
48

Figure 22: Session Termination (Online Charging)
Scenario described above assumes that the Mobile User notifies the serving ANP/TSP/VASP prior to disconnecting. However, in some cases Mobile User may logoff or terminates session suddenly, without notification. In order to ensure connectivity the 3P-AAA-Ping-Request/Answer messages will be exchanged. This mechanism of insuring that the connection is alive is employed by the Diameter base protocol. As stated in the Authentication, Authorization and Accounting Transport Profile (RFC3539) [36], peer should not disconnect until timer expires at least twice. Thus when the timer has expired twice and not reset, the ANP/TSP/VASP will deduce that the connection has been abruptly terminated and will signal a session tear down as demonstrated in Figure 24.
- The Mobile User device suddenly disconnects, for example, due to the device hardware failure. When this event occurs all other session participants are yet unaware of this failure.

- At some point, depending on the timer settings, the MU and the ANP/TSP/VASP exchange keep-alive messages in the form of the 3P-AAA-Ping-Request/Answer messages. Once the TSP/VASP notices that a 3P-AAA-Request message has not been responded to and the ping request timer has been expired twice, the TSP/VASP will initiate session termination. It will do so by first exchanging the final Credit-Control or Accounting messages.

- Once resource utilisation has been reported to the 3P-AAA server, Session-Termination-Request is sent to notify the 3P-AAA of the session tear down. On reception of the Session-Termination-Answer session is terminated.

- Down the line the ANP will notice that the user has disconnected and go through the same set of steps as the TSP/VASP.

- Once Mobile User will turn on the device, information about previously aborted sessions would allow user to issue a 3P-AAA-CDR-Request towards
the 3P-AAA server supplying Session IDS of the last ANP/TSP/VASP connections.

### 4.4.1.4 Phase 4: Re-Authentication and Re-Authorization

For variety of reasons, such as link failures or security related issues, Mobile user should be able to re-authenticate itself to the serving ANP/TSP/VASP and vice versa. Since X.509 Certificates have been previously exchanged, a 2-Way Authentication will be sufficient to re-authenticate entities to each other. In order to perform re-authorization, in cases when the online charging is used for the service in question, the 3P-AAA server will be consulted. Otherwise the ANP/TSP/VASP will make its own authorization decision. Figure 25 represents a case when the ANP wishes to re-authenticate and re-authorized. The same steps take place when the TSP/VASP wants to perform re-authentication and re-authorization.

![Diagram of ANP Re-Authentication and Re-Authorization](image)

Figure 25: ANP Re-Authentication and Re-Authorization (Online Charging)

Figure 26 describes an event where the ANP re-authorization has failed. Thus the MU/ANP session has to be terminated. Since Access Network is not available anymore, the current TSP/VASP session would have to be terminated as well. In case if the TSP/VASP re-authorization has failed, the TSP/VASP session termination will have no effect on the state of the ANP session.

- The ANP wants to perform re-authentication and re-authorization. Re-Authentication takes place through use of the X.509 2-Way Authentication procedure. Re-Authorization is a task performed by the ANP server in conjunction with a consultation as to the state of the MU’s account with the 3P-AAA server.
When either the ANP re-authentication or re-authorization has failed, the ANP/MU session has to be terminated. Due to the dependent nature of the TSP/VASP sessions on ANP’s transport, ANP’s session termination will force the TSP/VASP session to terminate as well.

ANP performing re-authentication and re-authorization will notify the Mobile User that it wishes to terminate session by sending 3P-AAA-Termination-Request specifying the reason for it within an AVP.

Next, the MU will notify the TSP/VASP and the TSP/VASP will go through the regular session termination procedure described in the previous section.

The ANP will perform its final Credit-Control message exchange, terminate session with the 3P-AAA server and then disconnect the MU session once it has received a 3P-AAA-Termination-Answer.

Once session is terminated, the user will issue a 3P-AAA-CDR-Request toward the 3P-AAA server.

4.4.1.5 Replenishing Account Credit

Often it might be the case that the Mobile User would run out of credit while accessing real-time charging resources of the ANP/TSP/VASP. When the Mobile User gets to the point of accessing his last credit units set aside, the Final-Unit-Indication AVP within the Credit-Control-Answer message should notify the user.
Once the Mobile User is aware that his/her credit is about to run out, the ANP/TSP/VASP would place restrictions on the access to the resource but the session will remain in the open state. Also it should be possible to replenish account as a single event through direct Mobile User to 3P-AAA-SP interface outside of any data access session. Mobile User simply sends a 3P-AAA-Credit-Request indicating the units that should be added to his/her account.

Four main scenarios may be distinguished here:

1) The ANP receives an update and the Mobile User buys more credit
2) The ANP receives an update and the Mobile User lets the Validity Timer to run out
3) The TSP/VASP receives an update and the Mobile User buys more credit
4) The TSP/VASP receives an update and the Mobile User lets the Validity Timer to run out

Since the decision taken by the Mobile User when ANP receives an update also triggers events at the TSP/VASP level, this scenario is reviewed in greater detail.

- In Figure 27 the MU is accessing ANP’s resource with the ANP periodically sending updates to the 3P-AAA to perform credit control monitoring. When the credit set aside is about to expire, the 3P-AAA will receive Final-Unit-Indication AVP.
- Reception of the Final-Unit-Indication AVP will trigger the ANP to send a 3P-AAA-Update-Request notifying the MU that the account has to be replenished.
- In the meantime the 3P-AAA server sets the Validity Timer and the ANP places restrictions on the use of its resources but not actually terminating the session.
- Since one of the possible outcomes of the signalling may be session termination, the MU informs the TSP/VASP that the final credit unit has been reached. Since ANP and TSP/VASP, depending on the service in question, set their account reservations separately, by the time the MU exhausts credit reserved for an ANP resource, credit reserved for a TSP/VASP resource might still be un-used.
- On the reception of a 3P-AAA-Update-Request from the Mobile User, TSP/VASP informs the 3P-AAA of the event and in turn receives the Validity Time from the 3P-AAA. Now the TSP/VASP places restriction on the use of its resources as well.
- Wishing to continue to participate in the session and to access ANP/TSP/VASP resources, the MU issues a 3P-AAA-Credit-Request to replenish account indicating the amount of monetary units. If transaction was
successful, the MU will be notified by the 3P-AAA server within corresponding 3P-AAA-Credit-Answer message.

- The ANP triggers authorization thus checking MU’s replenished account and reserving more credit. Once the ANP is happy with the results of the Credit-Control-Answer it will remove the restrictions imposed.
- The TSP/VASP will also perform authorization, receive Credit-Control-Answer and removed the restrictions. Since, while access was restricted, no session was terminated, the ANP/TSP/VASP sessions would retain their original Session IDs.
Figure 28 gives an example of an unsuccessful replenishment procedure. Just as in the previous scenario, the MU is accessing some online charging services. At some point the reserved credit is about to run out. And the ANP is notified of that.

In order to inform the MU that the credit replenishment is required a 3P-AAA-Update-Request messages is sent.

In the meantime the 3P-AAA server sets the Validity Time and notifies the ANP using a Credit-Control message. While account is not replenished, the ANP resources are restricted but the session is still active.
• The TSP/VASP service, having a different credit reservation instance, is still notified by means of the 3P-AAA-Update-Request of the possible ANP session termination. The reason for that is that the restriction placed by ANP has a direct effect on TSP/VASP session.

• TSP/VASP sends an update to the 3P-AAA server and receives the Validity Time set by the 3P-AAA. Now the TSP/VASP also puts restrictions on access to its services.

• In case if the Mobile User is unwilling to replenish credit by the time the ANP timer expires, ANP session termination procedure will take place.

• A 3P-AAA-TerminationRequest is sent out towards the Mobile User. Since TSP/VASP session cannot take place without ANP’s transport, the TSP/VASP session termination takes place first, followed by the ANP’s session tear down. Also since termination is triggered at ANP level and TSP/VASP has to follow suit or to perform vertical handover, it might be the case that when the MU/TSP/VASP session termination takes place some reserved units are still available and should be credited back to the Mobile User’s account by the 3P-AAA.

4.4.1.6 Failover Mechanism

Any infrastructure dealing with the accounting and collecting information related to charging should be able to handle connection failures and provide some sort of failover mechanism. One of the big advantages of the Diameter protocol in comparison to its predecessor RADIUS is that Diameter provides a failover mechanisms.

When the connection with the 3P-AAA server is lost any resilient network will have an alternative secondary server set up for storage of the session related data. In some cases that may not be possible when the routing of the messages is enforced to the specific fixed destination. Also it is stated by the Diameter Base protocol that the failover may produce a number of duplicate request messages and therefore care should be taken in detecting and removing these duplicates.

If the 3P-AAA server implementing Credit Control detects a failure during an ongoing session it terminates current session and returns the units reserved back to Mobile User’s account.

When the failure is detected by the ANP/TSP/VASP, i.e. the Credit Control client, two principal scenarios are possible. While the retry timer is running the ANP/TSP/VASP maintains session with the Mobile User and tries to reconnect with the 3P-AAA or to divert credit control and accounting data to an alternative server. Once the timer expires twice, depending on ANP/TSP/VASP implementation, it may
terminate session with the Mobile User or keep granting the service, locally storing the session related data and sending it to the server later when the connection is re-established. When this data is received by the 3P-AAA server, it will trigger ANP to send a 3P-AAA-Update-Request notifying the Mobile User that the data has been sent to the 3P-AAA server. Reception of the 3P-AAA-Update-Request will cause the Mobile User to send a 3P-AAA-CDR-Request to ensure that all the charges were applied properly.

Scenarios that may be considered, depending on the ANP/TSP/VASP implementation:

1) The ANP/3P-AAA interface connection has failed; TSP/VASP/3P-AAA is functional. ANP chooses to continue granting service, collecting and storing accounting data locally.
2) The ANP/3P-AAA interface connection has failed; TSP/VASP/3P-AAA is functional. ANP chooses to disconnect. This choice would affect the MU/TSP/VASP connection.
3) The TSP/VASP/3P-AAA interface connection has failed; ANP/3P-AAA is functional. TSP/VASP chooses to continue granting services.
4) The TSP/VASP/3P-AAA interface connection has failed; ANP/3P-AAA is functional. TSP/VASP chooses to disconnect.
5) Both ANP and TSP/VASP have lost connection to the 3P-AAA server.

Figure 29 displays signalling interactions when the ANP/3P-AAA interface connection fails and as a result sessions with the MU are terminated.

- During an on-going online charging session the ANP sends credit control update towards the 3P-AAA and receives no response. Also there is a mechanism embedded within the Diameter Base protocol that periodically checks whether connection is alive by means of the Device-Watchdog-Request/Answer messages. At some point the ANP will send new Device-Watchdog-Request and start timer waiting for response from the 3P-AAA. While timer is active session between the Mobile User and the ANP is active as well.
- The 3P-AAA server also periodically performs checks to ensure that the connection is still active. Having detected connection failure the 3P-AAA server disconnects and returns any unused reserved credit back to the MU’s account.
- Next the TSP/VASP session termination will follow the suit and complete its session. Since TSP/VASP still has connection with the 3P-AAA it would be able to complete the final Credit-Control in case if service implements the online charging or STOP accounting message to finalize accounting stream in case if the offline charging for this service is implemented.
- Since there is no connection to the 3P-AAA server, ANP cannot perform final Credit-Control update back to the server. However, unused reserved units have already been credited back to MU’s account.
- Once session has been terminated, the MU will send 3P-AAA-CDR-Request towards the 3P-AAA. Even if the ANP that was previously used for transport provision is unable to transport these messages to the 3P-AAA, there are
could be other ANPs within this area. If no alternative ANP is available, the MU will have to back off and try again later.

![Diagram of TSP Session Termination](image)

**Figure 30: Failover (ANP continues granting services)**

- In comparison to the previous scenario, Figure 30 shows signalling for an ANP, which will continue providing services to the Mobile User in case of the failover. Since ANP does not terminate, the Mobile User is completely agnostic as to the state of the ANP/3P-AAA connection. The MU will continue using whatever ANP/TSP/VASP services it had previously accessed.
- Once the Mobile User has finished utilizing resources, TSP/VASP session termination will take place as usual.
- Once the TSP/VASP session is over, if the MU does not want to access any other teleservices, ANP session termination will be signalled by means of a 3P-AAA-Termination-Request. Since there is still no connection to the 3P-AAA server and all of the Credit-Control information is collected by the ANP server, no final Credit-Control update can reach the 3P-AAA server.
- A 3P-AAA-Termination-Answer is issued by the ANP allowing the MU to terminate session. However, some AVP has to indicate to the MU
application’s state machine not to send a 3P-AAA-CDR-Request/Answer message toward the 3P-AAA server. The reason being is that even if an alternative ANP would be able to transport these messages to the 3P-AAA server, the information that the server currently holds is incomplete until it receives an update from the ANP.

- Once connection has been re-established, the ANP will forward all the charging or accounting information that it collected while connection was down. Once Credit-Control-Answer is received from the 3P-AAA server, the ANP will inform the Mobile User within a 3P-AAA-Update that now it can send 3P-AAA-CDR-Request. Once 3P-AAA-Update-Answer has been received, the ANP can disconnect.
- Having received an update from the ANP, the MU has been signalled that it can issue a 3P-AAA-CDR-Request towards the 3P-AAA server.

An observation can be made that in case when the connection fails between ANP/TSP/VASP and the 3P-AAA and ANP/TSP/VASP is implemented to provision services and accounting data storage, the charges generated may be greater than the actual credit available on the user’s account. When connection is re-established and charging data is forwarded to the server, the 3P-AAA would have to debit these charges from the user’s account. It might be a sensible idea to allow users to overdraw their accounts up to certain monetary amount.

4.4.2 HAC Related Scenarios

4.4.2.1 Introduction

One of the key issues that should be addressed within the context of heterogeneous networks is the handover techniques. Handover techniques can be viewed and classified according to a number of different parameters: soft and hard, vertical and horizontal, network controlled and mobile-assisted.

Hard handover is the type of handover that was typically employed by the analog telecommunication technologies and provides less flexibility and larger switching delays than the currently employed handoff techniques. It can be summarized that the hard handover technique is of the type break-before-make where current session will be disconnected and channel released and only then a new channel connection will be initiated. This technique is much easier to implement, however, it inhibits the problem of delays. Since nowadays channels do not only carry voice data where some delays and loss of data may be tolerated but also IP packets, this technique is not suitable due to its flexibility limitations. On the other hand soft handover finds alternative channel and initiates connection set up and only once alternative channel is available and ready for use, releases the old connection.
In older GSM networks the decision for handover was taken by the mobile operator. However with the growing importance of the QoS requirements, the need for a mobile-assisted handover emerged. With mobile assisted handover (MAHO) mobile equipment measurements have influence on the handover decision.

Another classification of handover can be seen from the perspective of the vertical or horizontal handover. Horizontal handover usually means that the mobile user changes its point of attachment without change of the access technology. Different horizontal handover mechanisms are implemented by different cellular and wireless technologies. Some scenarios may involve not only the change of the attachment point but also of the administrative domain. When Layer 3 (IP) handoff takes place, new IP address has to be allocated in the new domain. In general this distinction between what is considered to be user's Home domain and the Visited domain gives rise to differentiation in services available to the user and not only in the technical sense, but also differentiation in charges applied. UCWW proposes allocation of a single globally significant identifier (IPv6 address) [37] that will be associated with a user. This identifier will be used to gain access to teleservices regardless of the geographical location and to apply charges incurred.

Vertical handover is a relatively new concept that allows a single device to use multiple wireless interfaces to access network services. A number of currently available mobile devices are able to handle not only cellular networks but a number of other wireless access technologies such as WLAN, WiMAX and Bluetooth. Thus, within heterogeneous networks where a number of access technologies may be available to the mobile user the ability to switch between different access technologies is of paramount importance. In other words, teleservices available to the mobile user should be decoupled from the technology used to access them. Vertical handover can be divided into three principle phases: network discovery, handover decision and handover implementation. We will assume that the network discovery is outside the scope of this document.

Based on the above a number of conclusions can be made and applied to the HAC (Hot Access network Change) handover. The handover framework should be flexible implementing soft mobile-assisted handover and should be able to handle horizontal and vertical handoffs. As mention in [38] handover decision may be initiated by the Mobile User or the TSP/VASP entities when QoS fall beyond certain level guaranteed by the TSP/VASP or the ANP. Also it should be mentioned that for the purposes of this thesis what is important is the signalling application layer data generated during the handover procedure.

### 4.4.2.2 Vertical Handover Issues

At the moment one of the most robust architectures integrating cellular, WLAN and WiMAX access provisions is developed by the 3GPP. In general 3GPP architecture
closely follows the principles of loose coupling and high cohesion, where a number of elements perform very specific tasks. The issue of mobility and handover are closely woven. Previously mobility issues have been addressed at the IP level and a number of mobility solutions have been proposed: Mobile IPv6 [39], Hierarchical Mobile IP (HMIP) [40] etc. The downside of these schemes is the existence of the additional entities, such as Home Agent, and significant handover delays and overhead. Also due to the development of Internet a need for a new Transport protocol was emerging. SCTP protocol was introduced combining some of the properties of TCP and UDP with additional enhanced features suitable for modern day computing: multi-homing and multi-streaming. Combined with Dynamic Address Reconfiguration [41] extension SCTP can be used for seamless handover without additional functional entities. Using SCTP multi-homing feature and the ability to dynamically add/delete IP addresses to multiple device interfaces the mobile devices can move between different access networks maintaining its association with a remote server. Research has been carried out proposing different solutions [42-44] to vertical handover problem with slight alterations indicating the possibility of seamless handover with minimal service disruption.

4.4.2.3 User Triggered HAC

Scenarios described in this section form an important part of the overall user experience. One of the limitations of the current wireless/cellular networks is that once the user is connected to an ANP and accesses some services he/she does not have the ability to switch access technology on-the-fly and continue with an on-going session. In the context of UCWW when the Mobile User is within an area that has several access technologies, he/she should be able to switch an on-going session from cellular to wireless IP access if that change produces certain benefit from the financial and QoS level perspective. One of the possibilities is to include access service pricing information as an additional factor of the QoS metrics, i.e. QoS level variable can be composed of a number of physical parameters such as a bit rate, jitter, packet drop rate probability and a variable associated with the price. Depending on the type of the subscription with a 3P-AAA-SP this parameter may have different weight and thus have an influence on the choice of the ANP. Also care should be taken in the calculation of the QoS threshold as it may lead to a ping-pong effect where handoff signalling takes place back and forth thus producing unwanted overhead. User triggered HAC scenario can be envisioned when the MU, being connected to the ANP and accessing services provided by the TSP, may will to perform vertical handover switching to a different service provider. Typically, if the QoS level drops suddenly when accessing the service it should be the responsibility of the TSP/VASP to initiate HAC. Thus the most probable scenario for this case is when the Mobile User wishes to procure access to cheaper access coverage.
In Figure 31 the Mobile User has established an online charging session with ANP1 and establishes another session with TSP1. During this session the Mobile User is signalled that the QoS level has changed below certain threshold established or has received an update from the WBC notifying that another access network with higher QoS is available. The Mobile User chooses to perform the handover. The Mobile User initiates new connection to the ANP2 and goes through the initial process of Authentication and Authorization at the same time maintaining its current sessions with the ANP1 and the TSP1.

Once Authentication has been successful the Mobile User can avail of services provided by the ANP2. At the same time while connection to the ANP2 takes place, the TSP1 should be notified by means of the Update message that handover is about to take place, supplying identifier of the candidate access network.

When connection to ANP2 is established the Mobile User is currently connected to two access networks. Using the mSCTP (Mobile SCTP) features the Mobile User currently has multi-homed association with TSP1. Now stream of data can be reconfigured to take primary route path of the new ANP2 while closing the old ANP1 stream connection.
Since transport layer data has been successfully moved to the stream associated with the new ANP2, the Mobile User initiates Session Termination with the ‘old’ ANP1.

Closing of ANP1 session should have no effect on the session between the Mobile User and the TSP1, which continue to exchange the Credit Control messages.

4.4.2.4 TSP/VASP Triggered HAC

The TSP/VASP Triggered HAC describes the situation when the TSP/VASP server is not satisfied with the QoS level provided by the current access networks. When the Mobile User initiates session with TSP/VASP and accesses services, a certain level of QoS is guaranteed. If the access network is congested it would produce drop in the data rate and might not be satisfactory in term of required parameters for a teleservice. Thus in order to fulfil its obligations in terms of the QoS before its customer, the TSP/VASP would initiate the HAC procedure. In this case the extra charges that might be incurred when switching to an alternative access provider will be paid by the TSP/VASP.

- In Figure 32 the Mobile User has established session with ANP1 and TSP1 to access some teleservices. At some point the QoS of the teleservice falls beyond threshold level due to the access network problems. Since TSP1 is committed to provision of teleservice at certain QoS level it triggers the HAC procedure.
- Once decision is taken to perform HAC, the TSP1 notifies the Mobile User of its decision through an update messages signalling an alternative access network that the Mobile User should initiate connection to.
- Having indication of the handover procedure, the Mobile User will initiate another connection with the ANP2 by going through normal stages of a set up procedure that involves Authentication and Authorization steps. As indicated in [38] the Mobile User should include identifier of the ‘old’ ANP1 in its request messages.
- Once the Mobile User has received a new IP address from the ANP2 its Transport Layer can perform stream handover using mSCTP by dynamically adding the new IP address to the association. Once the new primary route has been set to include the newly assigned ANP2 address the ‘old’ ANP1 address can be deleted thus completing the soft handover of the data stream.
- In the upper layer the ANP1 Session Termination procedure takes place.
- Access to the teleservice provided by the TSP1 continues with consequent exchanges of the Credit Control information. It should be noted that the Credit Control exchanges related to the charges applied by the ANP2 are paid.
by the Mobile User but at the rate less than or equal to that of the ANP1. In case if extra charges were incurred during the HAC procedure, the TSP1, being the originator, will pay the extra-costs.

Figure 32: TSP/VASP Triggered HAC (Online Charging)

4.4.3 Novel 3P-AAA Scenarios

Flexibility of the 3P-AAA gives rise to the additional scenarios that might take place in UCWW:

- Switching teleservice provider during an on-going session
- Multiple ANP sessions when using teleservice(s) to enable asymmetric service delivery
- TSP chaining involving two or more TSPs and/or VASPS in provision of a teleservice to the user

4.4.3.1 TSP change

When discussing TSP-triggered HAC, first, classification of the teleservices should be established. Two principle types of services may be distinguished here:
1. Services that require disconnection of the old and initiation of the new session. Most of the teleservices would fall into that category. One of the issues here is that these services are stateful and the information about their state is of the local significance. Services such as web browsing (using cookies or tokens), location and presence services, games and data download would fall into this category.

2. Services where session is established with another Mobile User and may be handed over during an on-going session (Figure 33); this criterion would apply to voice or video transmission streams shared between participating nodes and applications such as VoIP or teleconferencing.

![Figure 33: User triggered HAC with TSP change](image)

Figure 34 demonstrates an example where the Mobile User is accessing some real-time charging teleservice:

- During an on-going session, the QoS level guaranteed by the TSP1 falls beyond allowed threshold value.
- While maintaining session with the original TSP, the MU is initiating a new connection with a service similar to the currently used but provided by the TSP2. The diagram above only covers signalling related to the 3P-AAA infrastructure. Any additional teleservice specific signalling is outside the scope of this description.
- If Authentication and Authorization steps are successfully completed by the MU, he/she can now access TSP2 service.
- Since new connection has been established, the session connection to the old TSP1 can now be terminated by invoking the session termination procedure.
- Once the TSP1 has been disconnected, sessions continue with the corresponding ANP1 and TSP2.
4.4.3.2 Multiple serving ANPs

Availability of several network access technologies in the given geographical region is a common modern day reality. Typically within metropolitan area a number of WAN, MAN and LAN access technologies would overlap. Since the whole idea of the 3P-AAA is to enable easy access, there should be provision to enjoy extended utilization of the available access resources. In case if the Mobile User is wishing to access services from TSP(s) in the region where multiple access technologies overlap, it should be possible to simultaneously have active sessions through different ANPs.

Figure 35 above demonstrates an example where MU1 is accessing services offered by the TSP1. Depending on the bandwidth requirements of each service accessed, media stream may be routed through two distinct ANPs with different access technologies. For example, delay sensitive real-time service traffic may be accommodated by the faster ANP. Decision to perform this kind of service access should also take into account the user subscription profile with 3P-AAA.
In technical terms the SCTP’s multi-homing feature may be used to provide stream delivery through different paths. At the moment, even though SCTP provides multi-homing capability where multiple paths may exist between source and destination, this feature is only employed for failover and retransmission. This limitation is due to the fact that these mechanisms have been inherited from TCP. However, since more and more emerging devices accommodate multiple network interfaces it is very probable that these issues will be addressed and resolved in the near future. Some SCTP schemes and multi-homing optimizations have been suggested in [45, 46].

When the Mobile User connects to some ANP, this ANP guarantees certain level of service that can be translated into some physical parameters such as bandwidth, throughput, queuing delays etc. At the same time accessing services provided by TSP, services also have some requirements in terms of physical and data link parameters. In case if a total requirement for services is greater than that provisioned by the currently serving ANP, two possibilities may be considered here:

- To look for an alternative ANP that would satisfy TSP’s requirements
- To establish session with another ANP and to distribute service access between newly connected ANPs

Some mechanism may be provided by the network to quantify physical aspects and to provide selection algorithm that would take into account not only physical parameters but also the customer’s profile preferences.

As an example consider scenario where the Mobile User is located in the area with N access network providers and is wishing to access K services offered by TSP(1). Assuming that QoS is some non-negative real number used to quantify parameters, following simple algorithm might be used:

1. Evaluate total resource requirements:

   \[ \text{QoS}_{\text{Total}} = \sum_{k=0}^{n} \text{QoS} \]
2. Compare resources available at the current ANP with resources required to satisfy all the requests
3. If amount of resources provided by the current ANP is less than the amount required, look for a minimal combination of N ANPs that would satisfy service requirements
4. Once found, distribute media flow between these ANPs

As can be noticed from Figure 36, in signalling terms, the message flow is similar to that of the user triggered HAC procedure for change of the ANP. The principle difference here is that instead of the session termination with ANP1, service delivery will continue through both ANPs.

**4.4.3.3 Service Delivery Chaining**

Flexibility presented by the 3P-AAA framework will influence expansion of the Value Added Service (VAS) supply since it would produce a more favourable environment for development and deployment of these services. Value Added Services may be defined as non-core services that provide some additional functionality to the basic services and may function as stand-alone services. VASPs provide greater service market diversification and specialization by targeting specific
group of customers. Often VASPs might require some additional resources for provision of their services.

Currently most of the VAS are implemented and deployed by the mobile operators. As a result, in order to gain access to some VAS and applications, a mobile user first needs to create a service level agreement with a mobile operator.

In [47] authors present good market classification and categorizations of m-commerce VAS offered by the Taiwanese mobile operators. This paper reviewed 40 service types with over 200 Value Added Service items offered by the mobile operators and classified them according to a number of criteria. The three major factors in the categorization are:

- The extent of dependence on the location
- The extent to which application is time critical
- Whether it is controlled by the mobile user or by the Service Provider

Based on the permutation of the above factors 8 possible arrangements may be produced:

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Information that is both timely and related to the immediate environment</td>
</tr>
<tr>
<td>II</td>
<td>Similar to I but controlled by the product or service provider</td>
</tr>
<tr>
<td>III</td>
<td>On-demand provision of information regarding physical environment of the recipient</td>
</tr>
<tr>
<td>IV</td>
<td>Similar to I but not time critical</td>
</tr>
<tr>
<td>V</td>
<td>Acquisition of time-critical information that is tied to a remote transaction</td>
</tr>
<tr>
<td>VI</td>
<td>Similar to V but initiative rests with information provider</td>
</tr>
<tr>
<td>VII</td>
<td>Receiver initiated information acquisition stored in a repository or database</td>
</tr>
<tr>
<td>VIII</td>
<td>Modification or configuration software for remote mobile users</td>
</tr>
</tbody>
</table>

In the above research most of the services fall within categories VI (182), IV (38) and I (13). However, the cases studied by this research are related to VAS offered by the mobile operator and not 3rd party VASPs. Also the 3GPP specifications provide examples of the types of services supported: SMS, MMS, Account Management, Terminal Status, Terminal Location, Multimedia Conferencing, Group List Management, Presence Services, Geocoding, Application Driven QoS, and Content Management etc.
One of the key ideas of the 3P-AAA framework is to stimulate teleservice diversity through decoupling of access and teleservice provisions. It is very likely that some of the value-added services already offered by the mobile operator would remain under the management of the access operator even in the UCWW, but it is going to be the new emerging teleservices and value-added services that would be mostly interested in the deployment within the 3P-AAA infrastructure.

Currently network operators are similar to the middle man between the 3rd party VASP and the end-user. Since charging and billing infrastructure has quiet strict implementation requirements, 3rd party VASPs utilize ANP’s infrastructure for these purposes. There are two business models in operation regarding the 3rd party VAS: VASP provider sells an application to an operator or VASP hosts an application and utilizes ANP’s charging infrastructure, thus the end user is billed by ANP on behalf of VASP.

As can be seen from the Figure 37 [48] a Service Delivery Platform (SDP) acts as a broker between VAS and Service Enablers. Once 3rd party VASPs registered with the SDP, its application will have access to Service Capabilities provided by the Service Enablers. Some 3rd party VAS may require more than one service capability from the network; these applications are called Composite Applications. As outlined in the 3GPP technical specification document regarding Open Service Access (OSA) [49], the principle tasks of the SDP are authentication, application registration, discovery and charging. Communication between these entities is handled by the OSA/Parlay Interface. Trying to put this framework in the perspective of the 3P-AAA, the following observation can be made:
Authentication procedure can be performed through exchange of X.509 Certificates

Services provided by the application as well as services offered by the Service Enablers may be registered and made discoverable through other UCWW entities (ADA activity [2])

Charging will be performed through the c interface connecting VASP and the corresponding 3P-AAA-SP

Thus SDP may be removed and replaced by the direct communication between 3rd party VASP requiring additional resources and the TSP/ANP offering them through an a interface.

Figure 38: Service Delivery Chaining Example

Figure 38 demonstrates an example where the MU1 is wishing to access services of the VASP1. This service may have been advertised through the WBC. Once session is established with the VASP1, the need for additional resources might arise for which TSP1 will be consulted. From the perspective of the TSP1, the VASP1 that is currently utilizes its resources is no different than the typical mobile client.

• In Figure 39 the MU1 has established a session connection with VASP1During this session the accounting and credit control data is exchanged between the 3P-AAA1 and VASP1 server. When the connection was established the VASP1 guaranteed provision of certain service with the corresponding level of QoS.

• If VASP1 requires some additional resources in order to successfully provide services, these resources can be purchased from the ANP or the TSP. At the moment, this kind of a framework exists within 3GPP IMS. To successfully fulfil its part of the service delivery, the VASP1 contacts the TSP1. Also in this case, mobile user is completely agnostic as to the interactions that happen between the VASP1 and the TSP1.

• Since the VASP1 and the TSP1 a priori do not share any security association, the Authentication and Authorization has to be first performed.

• If the Authentication and Authorization was successful, the VASP1 can now access resources of the TSP1. The TSP1 will maintain accounting and credit
control stream with the corresponding 3P-AAA1 to monitor resources consumed by the VASP1.

- As can be seen from the diagram, the three credit control streams exist in this scenario: between the ANP1 and the 3P-AAA1 on behalf of the resources consumed by the MU1, between the VASP1 and the 3P-AAA1 on behalf of the resources consumed by the MU1 and between the TSP1 and the 3P-AAA1 on behalf of the resources consumed by the VASP1.

Figure 39: Service Delivery Chaining

Figure 40 displays details of the session termination procedure when the service chaining is involved. Session termination procedure is similar to that of the normal session; the principle difference is that the additional signalling takes place to terminate session between the VASP1 and the TSP1.
4.5 3P-AAA and IMS integration

Services described by the UCWW framework are user-demand driven. In other words both SBM and CBM should be able to co-exist and occupy their corresponding niche in the market. It should be up to the users to evaluate and decide what services are better suited for their needs. Integration of 3GPP and 3P-AAA would allow mobile users to avail of services provided by both infrastructures. After making subscription with the 3P-AAA Service Provider and obtaining personal IPv6 address embedded within CIM (Consumer Identity Module) [37], the MU will be
able to gain access to the 3P-AAA services as well as to that of the user’s original Home Network.

Since the IMS has capability for provision of teleservices through the deployment of Application Servers and inclusion of VASP through the OSA infrastructure, it may be seen as an integrated access and teleservice provider. Deployment of the 3P-AAA framework will have an impact on the way teleservices are being offered not only from the point of view of the users but also of the TSPs. If previously TSPs and VASPs had to have a contractual relationship with the access network providers, now they could be considered as separate standalone entities. Thus, seeing the benefits offered by the 3P-AAA, any TSP/VASP that previously had a contractual relationship with the ANP would be able to break away and entrust its AAA management to a 3P-AAA service provider.

Consider a scenario where the MU is wishing to access some value-added service. Currently, the way to do this would be through the Home ANP. When the 3P-AAA is integrated with the existing IMS, as shown in the Figure 41 [50], MU will be able to establish session directly with TSP/VASP through the interface ‘a’.

![Figure 41: 3P-AAA and IMS integration](image)

### 4.6 Conclusion

This chapter has covered a lot of material describing different aspects of the 3P-AAA framework. The material presented here integrates certain technical aspects discussed in the previous chapters related to signalling and security. First, a higher level overview of the 3P-AAA framework was given. Since UCWW utilizes certain
concept-specific terms in the description of the framework, these terms are properly explained, e.g., ANP, TSP etc. The 3P-AAA signalling is at the core of the framework and most of the chapter is dedicated to the description of the transactions that take place by means of the envisioned interfaces. Each interface is designed to interconnect specific entities of the framework. In order to realize requirements needed for the implementation of the outlined interfaces, a number of scenarios and used cases have been reviewed. Basic signalling scenarios look at the interactions that take place when a single user is wishing to access single set of resources from the access- or tele-service provider. These scenarios include cases when both, online and offline, charging models are applied. In the cases involving handover, the new 3P-AAA specific HAC technique is outlined. In general, design of the 3P-AAA framework allows for the emergence of new signalling cases that would not be possible in the SBM world. These possibilities will have an impact on not only the way the mobile users access services, but also to the way these services are offered to them. Important thing to realize, is that the UCWW environment does not suggest complete removal of the legacy technology but rather a peaceful co-existence, where it would be up to the customers to decide which technology should become prevalent. The importance of this chapter is that it helped to identify messaging requirements that should be provisioned by the 3P-AAA signalling protocol. With the help of the case scenarios, these messages and their corresponding attributes will be formally defined in the next chapter.
CHAPTER 5

3P-AAA SIGNALLING

5.1 Introduction

Previous chapters have covered some technical background, where a number of signalling protocols have been mentioned. At the same time, chapter 4 looked at the different forms of interactions that might take place in the 3P-AAA environment. Based on the research outlined in the preceding chapters, this chapter sets out to formally outline the principle signalling messages and attributes required to fulfil the 3P-AAA signalling functionality. The first issue that would be addressed is what signalling protocol should be used as a foundation of the 3P-AAA signalling protocol. Good choice of the protocol is very important as it will have serious impact on the future performance of the framework implementations. Having chosen the right protocol and taking into account its format, new messages will be define to provide the minimal functionality of the 3P-AAA framework. In order to outline these messages in an orderly manner, first a set of messages for each interface of the 3P-AAA framework will be outlined, followed by the section summarizing all the new principle attributes related to these messages.

5.2 3P-AAA Protocol Stack

Previous sections have covered three signalling protocols that could be considered for implementation of the 3P-AAA: SIP [Section 2.8], PANA [Section 2.6] and Diameter [Section 3.3]. Table III below compares given protocols according to criteria listed on the left-hand side.

<table>
<thead>
<tr>
<th>Transport</th>
<th>SIP</th>
<th>PANA</th>
<th>Diameter Base</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SCTP, TCP, UDP</td>
<td>UDP</td>
<td>TCP, SCTP</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authentication</th>
<th>SIP</th>
<th>PANA</th>
<th>Diameter Base</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HTTP Digest AKA (in 3GPP), TLS X.509 certificate.</td>
<td>EAP negotiated (X.509 certificates proposed)</td>
<td>Application defined</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scalability</th>
<th>SIP</th>
<th>PANA</th>
<th>Diameter Base</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Scalable through SIP agents</td>
<td>Not scalable</td>
<td>Scalable through Diameter agents</td>
</tr>
</tbody>
</table>
Two principle approaches may be considered for the 3P-AAA implementation. The first approach can use the extended 3P-AAA Diameter for end-to-end signalling. 3P-AAA Diameter may use some of the PANA features to support authentication since both protocols have similar structure, where information is conveyed by means of AVP messages [51]. This approach would provide the AAA and Credit Control functionality for the three interfaces. In this configuration, the access router would operate as a Diameter Proxy, which is capable of modifying the message content and, therefore, provide value-added services, enforce rules and policy on different messages, or perform administrative tasks for a specific realm. This thesis adopts this approach and lists 3P-AAA messages and their corresponding AVP codes in the next section. Thus the protocol stack shown in Figure 42 will be adopted by the 3P-AAA signalling application [50]. Using the modular approach for the implementation of the protocol stack would allow for a more convenient maintenance or the addition of the new features.

The second approach can use SIP signalling between the MU and the access router, and Diameter on the inside of the network. Disadvantage of this approach is that the message translation would be required to extract information from SIP messages in order to form Diameter messages. However, some elements of this approach can be seen in the IMS, where Call/Session Control Function performs similar tasks. On the positive side, the use of SIP would provide a wider range of additional functionality as this protocol supports media stream negotiations and presence services.

The main reason why the 3P-AAA signalling protocol needs to borrow from other signalling protocols or to be based on them, is because this way the useful features of the underlying protocols can be re-used. This is especially important from the implementation point of view. Such features as resilience and error handling mechanism are especially important which makes the build-up of the new 3P-AAA features safer and more reliable when built on top of the protocols that have been widely tested and deployed in the industrial environment.
5.3 Messages and AVPs

Table IV below outlines the primary messages used in the 3P-AAA infrastructure per each interface. As can be seen from the table, messaging borrows heavily on the ideas outlined in PANA and Diameter Base and Credit Control Applications [51]. Most of the AVPs used in signalling have been outlined in the corresponding Internet Engineering Task Force (IETF) Request For Comments (RFC) documents. The newly devised AVPs and their details are listed in the following section.

<table>
<thead>
<tr>
<th>Messages over Interface ‘a’ (MU ↔ ANP/TSP/VASP)</th>
<th>Messages over Interface ‘b’ (MU ↔ 3P-AAA)</th>
<th>Messages over Interface ‘c’ (ANP/TSP/VASP↔ 3P-AAA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3P-AAA-MU-Initiation(3P-AAA User Application)</td>
<td>3P-AAA-Get-Credit-Request/Answer(3P-AAA User Application)</td>
<td>Credit-Control-Request/Answer(Diameter Credit-Control)</td>
</tr>
<tr>
<td>3P-AAA-Start-Request/Answer(3P-AAA User Application)</td>
<td>3P-AAA-Check-Balance-Request/Answer(3P-AAA User Application)</td>
<td>Re-Auth-Request/Answer(Diameter Base)</td>
</tr>
<tr>
<td>3P-AAA-Auth-Request/Answer(3P-AAA User Application)</td>
<td>3P-AAA-CDR-Request/Answer(3P-AAA User Application)</td>
<td>Session-Termination-Request/Answer(Diameter Base)</td>
</tr>
<tr>
<td>3P-AAA-Ping-Request/Answer(3P-AAA)</td>
<td></td>
<td>Abort-Session-Request/Answer(Diameter Base)</td>
</tr>
</tbody>
</table>
### 5.3.1 Messages over Interface ‘a’

#### 3P-AAA-MU-Initiation

MU uses this message to initiate session connection with an ANP or a TSP [17, 51]. It is assumed that the IP address of these entities is supplied through WBC service. This message is used to supply ANP or TSP with the MU’s identity. At this point Session-Id AVP is set to 0.

\[
3P-AAA-MU-Initiation ::= < 3P-AAA-Header: N >
\]

{Origin-Host} Section 6.3 of [27]

{Origin-Realm} Section 6.4 of [27]

{Destination-Realm} Section 6.6 of [27]

*[AVP]*

#### 3P-AAA-Start-Request

Once an initiation message has been received, ANP or TSP responds with a 3P-AAA-Start-Request message. Since X.509 Certificate will be required to mutually authenticate session participants, ANP/TSP sends its certificate in the start request message along with the session identifier allocated to the current session. In order to ensure message integrity during the session, ANP/TSP negotiate the integrity algorithm.

\[
3P-AAA-Start-Request ::= < 3P-AAA-Header: N,R >
\]

&lt;Session-Id&gt; Section 8.8 of [27]

{Origin-Host}
3P-AAA-Start-Answer

As response to the start request, corresponding node will reply to the ANP/TSP with a message that will contain its X.509 Certificate that will be used later during the Authentication procedure. Using integrity algorithm suggested by ANP/TSP, the MU will apply algorithm to the message load.

3P-AAA-Start-Answer ::= < 3P-AAA-Header: N >
<Session-Id>
{Result-Code} Section 7.1 of [27]
{Origin-Host}
{Origin-Realm}
{Destination-Realm}
{Certificate}
*{AUTH} 3P-AAA specific
*[AVP]

3P-AAA-Auth-Request

Authentication request message addresses the issue of mutual node authentication in the 3P-AAA environment. This procedure is based on the X.509 Certificates that were previously exchanged. Request messages will also include some session parameters, such as session timers and routing permissions, set by ANP/TSP and may also contain credit control and accounting AVPs.

3P-AAA-Auth-Request ::= < 3P-AAA-Header: N,R >
<Session-Id>
{Origin-Host}
{Origin-Realm}
{Destination-Realm}
{Nonce} 3P-AAA specific
{Event-Timestamp} Section 8.21 of [27]
{Digital-Envelop} 3P-AAA specific
{Service-Context-Id} Section 8.42 of [29]
{Session-Timeout} Section 8.13 of [27]
*{AUTH}
*[AVP]

3P-AAA-Auth-Answer
This message is used to carry information and AVPs related to the 3 way authentication procedure as well as the result of the authentication procedure.

3P-AAA-Auth-Answer ::= < 3P-AAA-Header: N >
<Session-Id>
{Result-Code}
{Origin-Host}
{Origin-Realm}
{Destination-Realm}
{Nonce}
{Event-Timestamp}
{Digital-Envelop}
{Session-Timeout}
{Service-Context-Id}
*(AUTH)
*[AVP]

3P-AAA-Ping-Request

Ping messages are used to check session’s aliveness and for failover mechanism purposes [17, 51]. Requests may be initiated by either MU or ANP/TSP. It is ANP/TSP that sets ping timer. Event-Timestamp AVP may be included here to provide some statistical data for trip delays etc.

3P-AAA-Ping-Request ::= < 3P-AAA-Header: N,R >
{Origin-Host}
{Origin-Realm}
{Destination-Realm}
{Ping-Timer} 3P-AAA specific
[Event-Timestamp]
*[AVP]

3P-AAA-Ping-Answer

This message is sent as a response message to a ping request.

3P-AAA-Ping-Answer ::= < 3P-AAA-Header: N >
{Result-Code}
{Origin-Host}
{Origin-Realm}
{Destination-Realm}
{Event-Timestamp}
*[AVP]

3P-AAA-Termination-Request
Message is used to indicate session termination procedure. This message can be originated by either MU or ANP/TSP. The reason for session termination is given in the Termination-Cause AVP.

3P-AAA-Termination-Request ::= < 3P-AAA-Header: N,R >
   {Session-Id}
   {Origin-Host}
   {Origin-Realm}
   {Destination-Host}
   {Destination-Realm}
   {Termination-Cause} Section 8.15 of [27] * [AVP]

3P-AAA-Termination-Answer

Message is send as a response to the termination request.

3P-AAA-Termination-Answer ::= < 3P-AAA-Header: N >
   {Result-Code}
   {Origin-Host}
   {Origin-Realm}
   {Destination-Realm}
   [Failed-AVP] Section 7.5 of [27] * [AVP]

3P-AAA-Update-Request

Update message is used as an informative message in the 3P-AAA Diameter application. It is used in scenarios related to credit replenishment, failover, handover etc. Since ANP session may have an impact on TSP session, for example, in cases when ANP has to be switched, update message is used to coordinate these actions.

3P-AAA-Update-Request ::= < 3P-AAA-Header: N,R >
   {Origin-Host}
   {Origin-Realm}
   {Destination-Realm}
   [Hot-Access-Change] 3P-AAA specific
   [Replenishment-Indicator] 3P-AAA specific
   [CDR-Notification] 3P-AAA specific
   * [AVP]

3P-AAA-Update-Answer

This message is issued as response to the update request.

3P-AAA-Update-Answer ::= < 3P-AAA-Header: N >
3P-AAA-Price-Enquiry-Request

This message is used to check price of access or teleservices [29, 51]. Must support AVPs defined by the Credit Control Application.

3P-AAA-Price-Enquiry-Request ::= < 3P-AAA-Header: N,R >
{Origin-Host}
{Origin-Realm}
{Destination-Realm}
{Service-Context-Id}
*[AVP]

3P-AAA-Price-Enquiry-Answer

This message is issued in response to the price enquiry request.

3P-AAA-Price-Enquiry-Answer ::= < 3P-AAA-Header: N >
{Result-Code}
{Origin-Host}
{Origin-Realm}
{Destination-Realm}
{Service-Context-Id}
{Cost-Information} Section 8.7 of [29]
{CC-Money} Section 8.22 of [29]
*[AVP]

3P-AAA-ReAuth-Request

Re-authentication request may be issued by either ANP/TSP server or the MU. Re-authentication may be performed by the MU before Authorization-Lifetime expires or issued by ANP/TSP server during account replenishment procedure. Since both corresponding entities possess their counterpart’s X.509 Certificates, 2 Way authentication is performed.

3P-AAA-ReAuth-Request ::= < 3P-AAA-Header: N,R >
<Session-Id>
{Origin-Host}
3P-AAA-ReAuth-Answer

Re-authentication answer sent as a response to the re-authentication request message.

3P-AAA-ReAuth-Answer ::= < 3P-AAA-Header: N >
   <Session-Id>
   {Result-Code}
   {Origin-Host}
   {Origin-Realm}
   {Destination-Realm}
   {Nonce}
   {Event-Timestamp}
   {Session-Timeout}
   {Error-Message}
   *[AUTH]
   *[AVP]

5.3.2 Messages over Interface ‘b’

3P-AAA-Get-Credit-Request

This message is sent directly to the 3P-AAA-SP and is seen as a request to allocate MU’s credit towards use of some ANP or TSP service. Variable units may be used for credit allocation such as time or monetary value.

3P-AAA-Get-Credit-Request ::= < 3P-AAA-Header: N,R >
   <Session-Id>
   {Origin-Host}
   {Origin-Realm}
   {Destination-Realm}
   {Service-Context-Id}
   {CC-Money}
   {CC-Service-Specific-Units} Section 8.26 of [29]
   {Cost-Unit} Section 8.12 of [29]
   {Currency-Code} Section 8.11 of [29]
   {Value-Digit} Section 8.10 of [29]
   *[AUTH]
   *[AVP]
3P-AAA-Get-Credit-Answer

Reply message to the credit request message.

3P-AAA-Get-Credit-Request ::= < 3P-AAA-Header: N,R >
  <Session-Id>
  {Result-Code}
  {Origin-Host}
  {Origin-Realm}
  {Destination-Realm}
  {Service-Context-Id}
  [Error-Message]
  *{AUTH}
  *[AVP]

3P-AAA-Check-Balance-Request

This message allows the MU to check his/her account balance.

3P-AAA-Check-Balance-Request ::= < 3P-AAA-Header: N,R >
  <Session-Id>
  {Origin-Host}
  {Origin-Realm}
  {Destination-Realm}
  {Service-Context-Id}
  *{AUTH}
  *[AVP]

3P-AAA-Check-Balance-Answer

A message sent as a response to the balance request. This message contains Result-Code AVP typical for Diameter requests as well as Check-Balance-Request defined by the Credit Control Application.

3P-AAA-Check-Balance-Answer ::= < 3P-AAA-Header: N >
  <Session-Id>
  {Result-Code}
  {Origin-Host}
  {Origin-Realm}
  {Destination-Realm}
  {Service-Context-Id}
  {Check-Balance-Result}Section 12.8 of [29]
  *{AUTH}
  *[AVP]
3P-AAA-CDR-Request

This message provides accounting and credit control transparency within the 3P-AAA framework. It is by means of this message that the customer is able to keep record of his/her resource usage. Every session initiated by the MU should have a corresponding Charging Detail Record.

3P-AAA-CDR-Request ::= < 3P-AAA-Header: N,R >
<Session-Id>
{Origin-Host}
{Origin-Realm}
{Destination-Realm}
{Service-Context-Id}
*(AUTH)
*AVP

3P-AAA-CDR-Answer

CDR answer is send as a response to the CDR request for this session. This message contains an Universal-3p3a-Charging-Detail-Record AVP as described in [38]

3P-AAA-CDR-Answer ::= < 3P-AAA-Header: N,R >
<Session-Id>
{Result-Code}
{Origin-Host}
{Origin-Realm}
{Destination-Realm}
{Service-Context-Id}
{Universal-3p3a-Charging-Detail-Record}
/Error-AVP
*(AUTH)
*AVP

5.3.3 Messages over Interface ‘c’

Messages identified in this section address communication between the Diameter Server and the ANP/TSP. These messages use Diameter Base [27] and Credit Control [29] defined messages with some additional 3P-AAA AVPs.

Credit-Control-Request

Message used to provide online accounting and credit control capabilities within the 3P-AAA infrastructure. Message is inherited from the Credit Control Application
and is exchanged between Credit-Control Client (ANP/TSP Server) and Credit-Control Server (3P-AAA Server).

Credit-Control-Request ::= < Diameter Header: 272,R >
  <Session-Id>
  {Origin-Host}
  {Origin-Realm}
  {Destination-Realm}
  {Auth-Application-Id}
  {Service-Context-Id}
  {CC-Request-Type} Section 12.5 of [29]
  {CC-Request-Number} Section 8.2 of [29]
  [ CC-Sub-Session-Id ] Section 8.5 of [29]
  [Origin-State-Id] Section 8.2 of [29]
  [Event-Timestamp]
  [Service-Identifier] Section 8.28 of [29]
  [Termination-Cause]
  [Requested-Service-Unit] Section 8.18 of [29]
  *[ Used-Service-Unit ] Section 8.19 of [29]
  [ Multiple-Services-Indicator ] Section 8.40 of [29]
  *[ Multiple-Services-Credit-Control ] Section 8.16 of [29]
  [HAC-Initiator] 3P-AAA specific
  *[AVP]

Credit-Control-Answer

Answer messages sent as a result of the Credit-Control-Request used in the variety of scenarios involving real-time accounting and credit control.

Credit-Control-Answer ::= < Diameter Header: 272 >
  <Session-Id>
  {Result-Code}
  {Origin-Host}
  {Origin-Realm}
  {Auth-Application-Id}
  {CC-Request-Type}
  {CC-Request-Number}
  [CC-Session-Failover] Section 12.6 of [29]
  [CC-Sub-Session-Id]
  [Acct-Multi-Session-Id]
  [Event-Timestamp]
  [Granted-Service-Unit]
  *[Multiple-Services-Credit-Control]
  [Cost-Information]
  [Final-Unit-Indication] Section 8.34 of [29]
  [Check-Balance-Result]
  [Credit-Control-Failure-Handling] Section 8.14 of [29]
  [Direct-Debiting-Failure-Handling] Section 8.15 of [29]
  [Validity-Time]
  *[Redirect-Host]
  [Redirect-Host-Usage]
  *[Proxy-Info]
  *[Route-Record]
Re-Auth-Request

This re-authentication request, in contrast to re-authentication described within interface a, is originated by the 3P-AAA server with intention of signalling to the ANP/TSP that the MU re-authentication should take place. This could be done for security reason when server session timer has expired.

\[
\text{Re-Auth-Request ::= < Diameter Header: 258, R >}
\]

\[
\quad < \text{Session-Id} >
\quad \{ \text{Origin-Host} \}
\quad \{ \text{Origin-Realm} \}
\quad \{ \text{Destination-Realm} \}
\quad \{ \text{Destination-Host} \}
\quad \{ \text{Auth-Application-Id} \}
\quad \{ \text{Re-Auth-Request-Type} \}
\quad \{ \text{Origin-State-Id} \}
\quad * \{ \text{Proxy-Info} \}
\quad * \{ \text{Route-Record} \}
\quad * \{ \text{AVP} \}
\]

Re-Auth-Answer

This message is sent as a response to the re-auth request by the corresponding party.

\[
\text{Re-Auth-Answer ::= < Diameter Header: 258 >}
\]

\[
\quad \{ \text{Origin-Host} \}
\quad \{ \text{Origin-Realm} \}
\quad \{ \text{Destination-Host} \}
\quad \{ \text{Destination-Realm} \}
\quad \{ \text{Failed-AVP} \}
\quad * \{ \text{AVP} \}
\]

Session-Termination-Request

Just like the termination request specified by the 3P-AAA Application, Diameter Session-Termination-Request is used to signal session termination to the corresponding node.

\[
\text{Session-Termination-Request ::= < Diameter Header: 275, R >}
\]

\[
\quad < \text{Session-Id} >
\quad \{ \text{Origin-Host} \}
\quad \{ \text{Origin-Realm} \}
\quad \{ \text{Destination-Realm} \}
\quad \{ \text{Auth-Application-Id} \}
\quad \{ \text{Termination-Cause} \}
\]
Session-Termination-Answer

Diameter session termination answer is sent as a response to the termination request.

Session-Termination-Answer ::= < Diameter Header: 275 >
< Session-Id >
{Result-Code}
{Origin-Host}
{Origin-Realm}
[Error-Message]
[Error-Reporting-Host]
* [Failed-AVP]
{Origin-State-Id}
* [Redirect-Host]
[Redirect-Host-Usage]
* [AVP]

Abort-Session-Request

Abort request may be sent by the Diameter server towards resources provider as a result of network failure.

Abort-Session-Request ::= < Diameter Header: 274, R >
< Session-Id >
{Origin-Host}
{Origin-Realm}
{Destination-Realm}
{Destination-Host}
{Auth-Application-Id}
{User-Name}
{Origin-State-Id}
* [Proxy-Info]
* [Route-Record]
* [AVP]

Abort-Session-Answer

Message sent as a response to the abort request.

Abort-Session-Answer ::= < Diameter Header: 274 >
< Session-Id >
{Result-Code}
{Origin-Host}
{Origin-Realm}
{User-Name}
Accounting-Request

Accounting messages would be typically used by the services and applications that do not require online charging. This message facilitates an exchange of the accounting data for resources and services used.

Accounting-Request ::= < Diameter Header: 271, R >
< Session-Id >
{Origin-Host} {Origin-Realm} {Destination-Realm} {Accounting-Record-Type} {Accounting-Record-Number} [Acct-Application-Id] [Vendor-Specific-Application-Id] [Acct-Session-Id] [Acct-Multi-Session-Id] [Acct-Interim-Interval] [Accounting-Realtime-Required] [Origin-State-Id] [Event-Timestamp] * [Proxy-Info] * [Route-Record] * [AVP]

Accounting-Answer

Diameter base accounting answer message is used to carry responses to the accounting request messages.

<ACA> ::= < Diameter Header: 271 >
< Session-Id >
{Result-Code} {Origin-Host} {Origin-Realm} {Accounting-Record-Type} {Accounting-Record-Number} [Acct-Application-Id] [Vendor-Specific-Application-Id] [User-Name] [Accounting-Sub-Session-Id] [Acct-Session-Id] [Acct-Multi-Session-Id]
[Error-Reporting-Host]
[Acct-Interim-Interval]
[Accounting-Realtime-Required]
[Origin-State-Id]
[Event-Timestamp]
* [Proxy-Info]
* [AVP]

**Disconnect-Peer-Request**

This message is used by the Diameter protocol to notify peer as to the reasons of the transport disconnection. As stated within the RFC 3588, the corresponding peer usually does not know the reason for disconnection and might assume it to be the result of the transport level failure with following periodic attempts to re-establish connection. Disconnect-Cause AVP, carried by the disconnect request, ensures that in some cases no action should be taken to re-establish connection.

Disconnect-Peer-Request ::= < Diameter Header: 282, R >
{Origin-Host}
{Origin-Realm}
{Disconnect-Cause}

**Disconnect-Peer-Answer**

Sent as a response to the disconnect request.

Disconnect-Peer-Answer ::= < Diameter Header: 282 >
{Result-Code}
{Origin-Host}
{Origin-Realm}
{Error-Message}
* [Failed-AVP]

**Device-Watchdog-Request**

Device Watchdog is an application level mechanism that is used to proactively detect transport failures. The exact mechanism is described in [36].

Device-Watchdog-Request ::= < Diameter Header: 280, R >
{Origin-Host}
{Origin-Realm}
{Origin-State-Id}
**Device-Watchdog-Answer**

This message is sent as a response to the device watchdog request.

Device-Watchdog-Answer ::= < Diameter Header: 280 >
   {Result-Code}
   {Origin-Host}
   {Origin-Realm}
   [Error-Message]
   * [Failed-AVP]
   [Original-State-Id]

**Capabilities-Exchange-Request**

These messages are used by Diameter to discover peer’s identity and capabilities. In case if corresponding peer does not share any common Diameter applications or security mechanisms, request originator will be notified of that through Result-Code AVP. It is also stated by the RFC 3588 that these messages must not be proxied, relayed or redirected. Since SCTP may be used as a transport protocol, this request should contain a Host-IP-Address AVP for each IP address that may be locally used when transmitting Diameter messages.

Capability-Exchange-Request ::= < Diameter Header: 257, R >
   {Origin-Host}
   {Origin-Realm}
   1* { Host-IP-Address } section 5.3.5 of [27]
   {Vendor-Id}
   {Product-Name}
   [Origin-State-Id]
   * [Supported-Vendor-Id]
   * [Auth-Application-Id]
   * [Inband-Security-Id]
   * [Acct-Application-Id]
   * [Vendor-Specific-Application-Id]
   [Firmware-Revision]
   * [AVP]

**Capabilities-Exchange-Answer**

Messages sent a response to the capability exchange requests.

Capability-Exchange-Answer ::= < Diameter Header: 257 >
   {Result-Code}
   {Origin-Host}
   {Origin-Realm}
   1* {Host-IP-Address}
   {Vendor-Id}
   {Product-Name}
   [Origin-State-Id]
   [Error-Message]
5.4 3P-AAA AVPs

Apart from the AVPs provided by the Diameter Base protocol and the Credit Control Application, some additional AVPs have been defined to support the 3P-AAA functionality. These AVPs have been drawn based on the requirements deduced from the signalling scenarios [53] as well as functionality of the PANA protocol [34].

**Certificate**

This AVP is of type OctetString and is used to carry X.509 Certificates [51]. This AVP is used in the authentication procedure and will accompany 3P-AAA authentication requests messages in order to provide certificate exchange between the corresponding parties.

**Integrity-Algorithm**

The motivation for this AVP is taken from PANA protocol where it is used to negotiate integrity algorithm between the party requesting resources and the party allocating them. Unlike PANA that states this AVP to be of type Unsigned32, in 3P-AAA this AVP is of type Enumerated as this type is easier to implement in software and the number of integrity algorithms used hardly requires the full range provided by a 32 bit space.

HMAC-SHA1-160  0
HMAC-MD5-128    1

**AUTH**

AUTH AVP is borrowed from PANA where it used to ensure message integrity [17, 51]. This AVP is of type OctetString and contains message authentication code calculated from the result of the concatenation operation between the session key and the signalling message load.
Nonce

This AVP is of type OctetString and is used to carry a pseudo-randomly generated number. Nonce is employed during the authentication procedure in order to enforce cryptographic reply protection.

Digital-Envelop

AVP of type OctetString used to carry symmetric session key generated by the ANP/TSP and encoded with MU’s public key [51].

Ping-Timer

AVP of type Unsigned32 used to set timing interval used by the 3P-AAA ping messages to check the aliveness of the connection.

Hot-Access-Change

Hot-Access-Change AVP is employed to provide additional information between signalling nodes during HAC handover. It is of type Grouped and has the following structure:

Hot-Access-Change ::= < AVP Header: N >
  [HAC-Initiator]
  [Multiple-ANP-Provision]
  *[Old-Service-Provider]
  *[New-Service-Provider]

HAC-Initiator

An auxiliary type DiameterIdentity HAC AVP used to indicate the party that initiate the handover procedure. It is important for charging related information as the party that initiated HAC would be responsible for possible access charges.

Multiple-ANP-Provision

To provide grater flexibility and higher QoS, in some cases, depending on the MU’s subscription profile, it might be possible to employ multiple ANPs at the same time to ensure higher quality and rate of access. This AVP of type Enumerated is used to indicate to the ANP/TSP whether this type of provision is enabled.

MULTIPLE-ANP-PROVISION_ALLOWED 0
Old-Service-Provider

This AVP of type DiameterIdentity is used to signal the identity of the service provider, ANP or TSP, which is being switched.

New-Service-Provider

This AVP of type DiameterIdentity is used to signal the identity of the new service provider, ANP or TSP, towards which new session is being initiated by the 3P-AAA client.

Replenishment-Indicator

This AVP is of type UTF8String and contains value of the Service-Context-Id. It is used by the update message to indicate that further credit should be allocated to this particular service.

CDR-Notification

AVP of type Grouped employed by the update message in the scenario when due to disconnection with the 3P-AAA server, MU was not able to receive CDR. In this case, the service provider should notify the MU that connection was re-established and CDR should be requested.

\[
\text{CDR-Notification} ::= \langle \text{AVP Header: N} \rangle
\]
\[
\{\text{Session-Id}\}
\]
\[
\{\text{Service-Context-Id}\}
\]

Universal-3p3a-Charging-Detail-Record

This AVP of type UTF8String contains charging detail record for each session. Charging Detail Records are used to enforce accounting and credit control transparency.

Termination-Cause

This Enumerated type AVP is part of the Diameter Base protocol and is used to convey the reason for session termination. Since some additional scenarios have
been outlined that are not provisioned by the original protocol, additional clauses should be added to the message.

3P-AAA_NO_TRANSPORT  9
3P-AAA_HAC  10

5.5 Conclusion

Chapter 5 completes the 3P-AAA background research and design stage of the project. Previous chapters have provided information related to the technical details of the available signalling protocols and security mechanisms, the 3P-AAA framework layout and interface description culminating in the description of the 3P-AAA protocol, its protocol stack and the corresponding protocol messages.

In order to avoid definition of a completely new signalling protocol, which would require a significant research effort, this thesis chose to consider other application level signalling protocols that could be used as a base for the design of the 3P-AAA signalling. After thorough review of the candidate protocols, it was decided that the Diameter Base protocol would form basis of the 3P-AAA signalling also borrowing functionality of the PANA’s authentication. These two protocols can be combined together due to the similarity of its messaging formats. Use of Diameter would also allow implementation of the online and the offline charging using the Diameter Credit Control and Accounting. Additionally, in order to satisfy requirements for the novel interactions scenarios outlined in chapter 4, new messages and attribute-value pairs were defined. These messages were defined for each interface of the 3P-AAA framework.
CHAPTER 6

IMPLEMENTATION ISSUES

Careful architectural design is of paramount importance from the project management point of view as it allows to minimize implementation time and helps to eliminate certain conceptual errors. This thesis primarily addressed 3P-AAA design issues through careful examination of the framework architecture and signalling protocols. This section looks at the possible implementation methods that could be adopted for the creation of 3P-AAA infrastructure. The following protocol stack implementations will be discussed:

- OpenDiameter open source project [54]
- OpenBlox Diameter Base stack by TraffixSystems [55]
- JDiameter open source project from the Java.net community [56]
- Cpana open source project [57]

Additionally some licenced versions of the Diameter protocol stack will be mentioned: IntelliNet’s Accelero [58] and Marben’s Diameter [59]. Also some issues related to the possible 3P-AAA framework simulation will be outlined, where the principle tool is the Network Simulator 2 and 3 (NS2/3) [60, 61]. Based on the material discussed in this chapter recommendations will be made concerning implementation of the 3P-AAA framework.

6.1 Protocol Stacks

Software implementation of the Diameter Base protocol is needed to provide even basic implementation of the 3P-AAA signalling capabilities. Since Diameter is widely used in the IMS infrastructure, the biggest testing ground for this protocol has been organization of the IMS/NGN Plugfests. These events have been organized to bring together leading IMS and NGN software vendors, systems integrators, and service providers delivering cable, wireless, wireline and enterprise solution in order to see in what state the industry is currently in regarding IMS rollout and to ensure interoperability between different vendors. Up to date, eight Plugfest events have taken place where each event has been centred on specific set of issues. Based on the Plugfest results and findings, Forum’s Technical Working Groups publish white papers outlining IMS/NGN best practices and guidelines. A number of commercial stack implementations are available [62], IntelliNet’s Accelero and Marben’s
Diameter stack being examples. However, the protocol stack implementations offered by these companies do not provide access to the source code and only offer binary files. The problems with that is that even though new attributes and messages can be defined, the state machine cannot be modified and thus the interactions outlined in chapter 4 cannot be integrated. Another down side of the commercial software is its licence price.

### 6.1.1 OpenDiameter

OpenDiameter was the first open source implementations of the Diameter Base protocol. This stack has been developed in 2004, shortly after emergence of the protocol itself. It is based on a number of C++ libraries that are currently supported by Linux and Windows platforms. EAP and PANA protocols are also part of the OpenDiameter project. EAP stack supports a number of methods, such as EAP-MD5, EAP-TLS etc.

Core OpenDiameter libraries of the latest release are listed below:

- ibdiamparser: Diameter message parser library (with XML dictionary support), with capable of user-defined AVP type parsers
- lib Diameter: Diameter core engine library with base accounting support.
- lib Diametereap: Diameter EAP Application library
- lib Diameternasreq: Diameter NASREQ Application library
- libeap: EAP library
- lib Diametermip4: Diameter MIPv4 library
- EAP-Archie: A key-derivative EAP authentication method implementation
- EAP-TLS: A key-derivative EAP authentication method implementation (for Linux/FreeBSD only)

The OpenDiameter C++ API is a simple session based API with each type of Diameter session being represented by a C++ class. User applications derived from these session classes to implement their own specific AAA functionality. All events, message processing and message transmission functionality are provided by these classes. Generally, the session classes are categorized into either client or server. The client classes provided AAA client capabilities and server classes provide AAA server functions. These two types of classes are further sub-divided into either authentication/authorization classes and accounting classes.

The information stated above is listed in the OpenDiameter documentation. Even though OpenDiameter is widely used for research in academic community, it is very hard to find any coherent and truly in-depth information on its installation and use. Project’s web site [54] contains OpenDiameter project documentation, however, it is
poorly maintained and rarely updated. One of the problems is that Open Diameter itself depends on the number of other open-source software packages. The main prerequisites stated in the installation notes are:

1. GNU g++ used to compile the C++ libraries
2. Xerces C++ XML parser version 2.1.0 and higher that is used for parsing Diameter messages
3. ACE Library 5.5.0 Adaptive Communication Environment (ACE) is a freely available, open-source object-oriented (OO) framework that implements many core patterns for concurrent communication software.
4. Boost Library free peer-reviewed portable C++ source libraries
5. OpenSSL Library that implements the Secure Sockets Layer and Transport Layer Security

Some versions of the prerequisite software are conflicting with each other. It is stated that OpenDiameter can run on Linux as well as Windows 2000/XP, at the same time documentation warns against Windows installation claiming it to be unstable. Overall, installation of the software is very problematic not to mention development which requires very high level of programming expertise.

**6.1.2 OpenBlox**

OpenBlox Diameter Stack is offered by the TraffixSystems which is one of the companies that actively participates in the IMS/NGN Plugfest events. Unlike OpenDiameter, which is only available in C++ implementation, OpenBlox is available for C++ and Java platforms. Apart from implementation of the Diameter Base, the company also provides support for 55 interfaces standardized by the bodies like 3GPP, ETSI (European Telecommunication Standard Institute) and WiMax [55]. OpenBlox software along with interface implementation is available freely with an option of getting additional interfaces and software support with purchase of the licence. The fact that OpenBlox is software that has been tested in the industrial environment makes it more reliable and better maintained than the OpenDiameter. However, the problem with OpenBlox is that the services offered by the open software licence do not allow access to some parts of the program implementation and do not provide documentation outside of the basic interface set. Licensed version of the software, which includes additional interfaces, support and training, is well outside the financial reach of our academic project.

**6.1.3 JDiameter**

Another Diameter Base protocol implementation that was available in the open source development community is JDiameter that was offered as a Java implementation of the stack and whose libraries were available for download. The
site that hosted the project (www.Java.net), hosts a number of open source software projects implemented in Java. However, it seems that the project has been removed from the hosting website.

6.1.4 Cpana

Cpana is an open source software that implements PANA protocol in C programming language. The project is registered on the sourceforge.net from the August of 2010 [57]. As outlined in the README document attached to the project installation, Cpana contains the following code:

- cpana - PANA library
- ceap - EAP library
- clpe - library containing common miscellaneous functions for cpana and ceap.
- apps - contains example applications including cpaa (PAA) and cpac (PaC)

Looking at the documentation supplied by the project, it becomes evident that this implementation might not be very suitable for adoption due to the following reasons:

- this implementation only partially adheres to the underlying PANA and EAP standards
- the software documentation is very limited
- implemented programming language is very platform depended with the Cpana software written specifically for Unix adherent Linux and BSD platforms

6.2 Simulation Issues

Network simulation is a common technique that is used to test some behaviour of the real network virtually. Even though simulation can only be considered as an approximation to the real world environment, it is considered to be inexpensive and fast in the provision of useful quantitative metric regarding the abilities of the network. In the case of the 3P-AAA some parameters of interest would be the ones related to the signalling latency, scalability and responsiveness of the infrastructure. The most common tool used in the academic research is Network Simulator (NS) 2 [60] and the newer version NS 3 [61]. NS2/3 is open source software that provides a virtual simulation environment. It uses C++/Python written libraries to simulate some common protocol stacks for different levels of OSI stack. It also uses Object Tcl (OTcl) scripting to set up the simulation environment. The problem of NS2/3 is that it does not have Graphic User Interface (GUI) and requires certain level of expertise and understanding of scripting languages. A 3P-AAA simulation would require use of protocols such as mSCTP and 3P-AAA Diameter that are not available
in either version of the NS and thus have to be written from scratch. In general, developing this thesis we tend to have an abstract look at the lower levels of the OSI protocol stack. Simulation may help to evaluate how interactions and different scenarios involving different access technologies might influence the overall performance of the system.

### 6.3 Conclusion

Currently available protocol stacks are not well suited for the project implementation. One of the drawbacks of the OpenDiameter and Cpana is that both of these software packages are written in C/C++, languages that heavily depend on the underlying OS platforms. The source code produced is constrained to run on only limited set of the operation system environments typically Unix based, which seriously hinders portability. The solution to that problem would be to implement the 3P-AAA protocol in Java, which allows software to run on any device with a compatible Java Virtual Machine. Most of the modern handheld devices like mobile phones, smart phones, reading pads and laptops support JVM environment.

Since 3P-AAA introduces new features and scenarios that are not possible for most Diameter implementations, adaption of the new protocol outlined in chapter 5 would require changes to the protocol’s state machine in order to accommodate interaction scenarios described in chapter 4. Currently, none of the available of-the-shelf protocol stacks are suitable for this task. The reason being that the available software was developed to adhere to the common IETF or 3GPP standards that do not envision interactions outlined in the 3P-AAA framework. Probably, some of the libraries used by the open source software could be used as reference models, but in general in order to create the environment outlined by the 3P-AAA a totally new 3P-AAA-tailored software would have to be written from scratch.

Based on the description of the issues above, a statement can be issued that the implementation of the 3P-AAA signalling protocol would require good technical knowledge and experience in C++/ Java programming as creation of the new robust software is a non-trivial matter.
CHAPTER 7

CONCLUSIONS AND FUTURE WORK

The main goal of this thesis was to set out the reason and the challenge of creating a new 3P-AAA infrastructure, and to demonstrate and discuss different aspects of the envisioned 3P-AAA infrastructure. That includes not only the details of the framework, like signalling protocols and participating entities, but overall motivation and reasons for the emergence.

As outlined in the introduction chapter, it is important to realize that the proposition made by the development of the 3P-AAA goes well beyond technological innovation. It gives a new perspective at the service offering in general. All the business models currently adopted in the telecommunication industry are built on the foundation of the subscription environment. Even though new business models introduce some form of innovation, their flexibility is inherently constrained by the structural limitations. 3P-AAA aims at removing these barriers through adoption of the Consumer-centric Business Model. Instead of the multiple subscriptions with numerous service offering entities, CBM requires only single entity to provide Service Level Agreement subscription - that of the 3P-AAA Service Provider. 3P-AAA-SPs will specialize in offering their services to a number of clients that would encompass ANPs, TSPs and, of course, Mobile Users.

This novel UCWW environment created by the combination of the CBM and 3P-AAA adoption will introduce a number of new scenarios and benefits that are not currently available to the typical end client. In this environment every mobile client would be able to enjoy full spectrum of services offered by the telecommunication industry. This includes control over the choice of the access provider services as well as numerous value added services whose offering will not depend on the underlying infrastructure of the access providers. This also invokes a number of benefits for the smaller and middle sized service providers. In general development of the charging and billing infrastructure is a complicated and money-demanding process. Decoupling of the charging and billing services from the underlying service provision would provoke a more active participation in the market of smaller service offering entities. This in turn would create a more competitive and thus more customer-beneficial environment centred on the end user demand.

Having outlined the principle goal of the 3P-AAA environment the question arises as to how these changes and environment can be accommodated. Chapter 2 performs an overview of the available technologies and frameworks that could be used as points of reference for the 3P-AAA development. Design of the 3P-AAA should include strong security features as well as robust and flexible modes of operation. 3P-AAA
uses a number of security related technologies such as IPsec, TLS and X.509 Certificates. The latter is used primarily for the user authentication in the wireless environment.

Communication between participating entities is of paramount importance for success of the project. Here the principle role is played by the appropriate choice of the signalling protocol as well as careful review of the salient features. A number of signalling protocols exist in the telecommunication industry; the most popular ones are RADIUS, SIP and Diameter. PANA is another protocol that has much to offer, however it is still not adopted by the industry and requires a more careful research and scrutiny from the academic community. Signalling employed by the 3P-AAA evaluates features of these protocols. Some additional features outlined by 3P-AAA are a novel vertical handover technique- Hot Access network Change (HAC). HAC enables Mobile User to make handover decisions based on the QoS levels of the access or teleservice in question. This may include cases of handover even when MU is not moving and is simply unsatisfied with the current service provision. In order to facilitate handover process at the lower levels of the OSI stack, it is considered that the transport profile of the SCTP with an extension that allows dynamic IP interface assignment should aid the handover process. Another feature that worth mentioning is that 3P-AAA signalling will provide direct communication between MU and serving 3P-AAA-SP. That signifies that services related to the account access will be accomplished directly through this interface and would include features like credit check, account top up etc. As a result of technical review of frameworks and signalling protocols, available and salient features are integrated into case scenarios. Later, based on these scenarios technical specification for 3P-AAA signalling is drawn with description of the messages and corresponding AVPs.

Of course, in real terms, every emerging technology should have provisions for integration and backward compatibility with legacy frameworks. This thesis looks at the possible co-existence between 3P-AAA framework and another 3G technology that is currently gaining momentum in the telecommunication industry- IP Multimedia Subsystems. IMS definition is a work of the 3GPP consortium and its main achievement is the decoupling of the access, control and service planes. IMS and 3P-AAA frameworks could possibly coexist in the telecommunication environment making it up to the user and other participating entities to decide what technology will be prevalent.

Diameter protocol with some adaptation is the principle protocol envisioned for 3P-AAA signalling. The chapter covering Diameter Base protocol has plenty of technical details but one of the most useful features of Diameter is its extensibility. Diameter Base framework is adopted by a number of other protocols as can be seen from the list of the available Diameter based applications. Maintenance and revision procedures always require significant effort in the IT industry. It is especially important for 3P-AAA signalling framework since a number of design features and
scenarios might have to be revised, altered or added during transition between design and implementation stages of the project.

The following section contains description of the future work for the project:

- Implementation of the 3P-AAA signalling- as discussed in the implementation issue section of the thesis, implementing 3P-AAA signalling possesses some serious challenges. Since protocol defines behaviour not outlined in the Diameter Base protocol and thus requires review of the state machine, 3P-AAA signalling implementation cannot use Diameter Base stack implementations currently available. Unless new software will emerge that allows redefinition of the state machine, it might be the case that the protocol will have to be implemented from scratch based on the requirements.

- Alternative SIP/Diameter Implementation- SIP is widely used for front-end signalling within IMS. It also provides a number of extended session control features well-suited for multimedia sessions. It might be beneficial to investigate the possibility of the front-end signalling involving SIP and back-end signalling involving Diameter. The disadvantages of this approach would be additional need for translation of received SIP messages into corresponding Diameter format. However, experience in that field can be borrowed from the IMS implementations. Also, this approach might be more appropriate for integration of IMS and 3P-AAA environments, since it would require minimal changes in the IMS signalling.

- Framework Simulation- with the creation of the 3P-AAA signalling application, simulation would have to be performed in order to provide some feel as to the functional environment of the framework. Simulation will also enable collection of some quantitative data. A choice of the appropriate simulation tool would have to be made. Common tools include NS2/3 and OPNET [63]. However, since 3P-AAA does not use standardized upper level protocols (Diameter extended 3P-AAA protocol and mSCTP), simulation would require additional technical expertise for the development of the additional libraries in order to simulate operational environment.

- Test Bed development- Simulation produces only approximated results of the real world operating environment. Even though simulation may provide better and cheaper scalability, for this project simulation would require extensive development effort. Thus a better approach might be the test bed development. Test bed might provide a useful inside in the operations of the overall framework and help to collect some useful data. Since it is hard to make predictions about physical performance parameters a priori, process of the overall interactions between different levels of the OSI stack should be monitored. These interactions may have a profound influence on the physical channel parameters such as signal latency when tested in the normal operating scenarios versus HAC involved operating scenarios.
Another issue that should be addressed, especially considering the importance of the charging data produced, is testing different security features and profiles. This may include strength of the X.509 Certificates along with additional IPsec and TLS features and how these additional features affect round-trip delay time.

- Design Re-evaluation- based on the results of the protocol implementation and test bed simulations overall re-evaluation of the design should be performed. This re-evaluation should address three prominent issues:
  - Possible changes to the 3P-AAA signalling protocol might include features built into the protocol itself. For example, use of the asymmetric cryptographic methods might be too costly or latent in the wireless environment. Some other cryptographic methods or combination of methods might be considered.
  - Overall evaluation of the protocol stack composition might signal some problems with the current design of the protocol stack, i.e. the combination of different layers of the OSI stack. For example, in order to accommodate vertical handover for HAC related scenarios SCTP was adopted due to its multi-homing features. In case if this transport profile shows poor performance, some other possibilities might be considered, i.e. UDP/TCP protocols in the Transport layer and MIPv6 [64] or HMIP [40] in the IP layer.
  - Optimization- in order to improve overall performance and to minimize signalling overhead, some optimizations to the original design should be considered. One possible optimization in order to minimize constant communication with the back-end server could be collection of the accounting/charging data at the local service providing entities that will later be sent over to the 3P-AAA-SP. Another possible optimization is temporary storage of the X.509 Certificates in order to minimize signalling for service providers that are often accessed by the same Mobile User.

- In case if implementation produces good results and after careful re-evaluation of the original design, the next logical step would be standardization of the 3P-AAA interfaces through formal submission of the Request For Commence (RFC) document to the Internet Engineering Task Force (IETF) standardization body.

**Research outcomes published to date**

- Dmitry Tairov, Ivan Ganchev, Máirtín O'Droma et al. (University of Limerick, Ireland). Ubiquitous Consumer Wireless World- Protocols Foundations and Standardization. URL: [http://www.globeforum.com/dublin](http://www.globeforum.com/dublin). This poster was presented at the Globe Forum Dublin, November 17, 2010
[35] The poster outlined basic infrastructural layout of the 3P-AAA framework along with its primary entities and interfaces.

- Dmitry Tairov, Ivan Ganchev, Máirtín O’Droma (University of Limerick, Ireland). Ideas on a third-party authentication, authorization and accounting framework and associated signaling scenarios for a ubiquitous consumer wireless world. TD(11)011. URL: http://cost-winemo.org/tds.html. This paper was presented at the 3rd meeting of European Science Foundation’s ‘COoperation in the field of Science and Technology research action on Wireless Networking for Moving Objects, WiNeMO, COST IC0906 [65], February 15, 2011, Riga, Latvia. The presentation described business model motivation for the emergence of the 3P-AAA infrastructure along with technical details of the framework design, IMS integration concerns, signalling and HAC handover concepts.

- Dmitry Tairov, Ivan Ganchev, Máirtín O’Droma (University of Limerick, Ireland). Third-Party AAA Framework and Signaling in UCWW [50]. This paper was accepted for the upcoming IEEE 7th International Conference on Wireless Communications, Networking and Mobile Computing, September 23-25, Wuhan, China. URL: http://www.wicom-meeting.org/2011/. This paper looks at the design of the 3P-AAA signalling protocol and investigates what currently existing signalling protocols could be used as a foundation of the signalling infrastructure.

- Dmitry Tairov, Ivan Ganchev, Máirtín O’Droma (University of Limerick, Ireland). Signaling messages and AVPs for 3P-AAA framework [53]. This paper was accepted for the upcoming IEEE 5th International Conference on Next Generation Mobile Applications, Services and Technologies, September 14-16, 2011, Cardiff, Wales. URL: http://www.ngmast.com/. Based on the work related to the anticipated signalling scenarios envisioned for the 3P-AAA framework, this paper looks at the requirements of each signalling interface and outlines the 3P-AAA signalling protocol stack along with new protocol messages and their corresponding attributes.
REFERENCES


